From: Aaron Turrill
To: Assistance Bill Consultation
Subject: Submission to consultation on the Assistance and Access Bill 2018
Date: Thursday, 6 September 2018 1:07:28 AM

Dear Minister,

I am writing to express concerns regarding the draft legislation titled 'The Assistance and Access Bill 2018'.

My first concern relates to the ability of the Australian Government to compel technology providers to provide assistance in the form of tools or mechanisms that provide access to systems. I find this concerning as:

1. This would reduce the security integrity of systems that Australians and other citizens use given that the broad scope of the Act may permit untargeted tools to cause collateral damage and affect Australian citizens;

2. This would, in turn, increase the probability of a high profile cyber attack that could;
a. Potentially expose sensitive information, eg. Tax File Numbers or bank account access details,
b. Cause economic damage to the citizens, corporations, or government of Australia,
c. Cause damage to infrastructure or other core systems owned, operated or critical to Australia, and
d. Reduce confidence in government or technical institutions.

Whilst I acknowledge that certain steps may be taken to protect the citizens of Australia, my second concern is that the measures the Act permits are only limited by what the Attorney General considers “reasonable and proportionate”.

Whilst the Attorney General must be satisfied that the technical capability notice must be "practicable; and... technically feasible", the technical skill of the Attorney General is likely insufficient to make such a judgement; in many cases, ICT product is exceptionally complicated and may involve complex interplay between hardware, firmware and software that can only be understood by a technical expert that regularly works with the ICT product. Whilst there are experts in the Australian Government (ie. ASD and related organisations), these technical personnel may also lack necessary experience with specific ICT products or may have motive to misrepresent the effect of a technical capability notice.

Government workers have been observed to abuse telecommunications access powers, with Australian Federal Police officers gaining unauthorised access to data [1]. Whilst this is an outlier case that involved circumventing the legal process, a lack of judicial oversight to the technical capability notice may provide a malicious actor greater leeway in escaping oversight should a fraudulent technical capability notice be issued.

Given the potential risk in approving a technical capability notice and the possibility for abuse, there should be greater judicial oversight in this process. Other countries have incorporated judicial oversight into similar processes to ensure democratic processes are not undermined; there is no valid reason for Australia not to follow suit.

My third concern is that the Act will not provide any significant benefit in the long term for the increased risk that it creates. Whilst 'black box' systems such as Microsoft Windows, certain networking hardware and other ICT products may permit alteration

without the end user's knowledge, open source systems such as GNU/Linux variants and the Android Open Source Project [2] as well as open source encryption software such as OpenPGP [3] and Open Whisper Systems [4] are publicly auditable for alterations inserted as part of a technical capability notice. Whilst many ordinary Australians do not care significantly about the security of their devices or applications, malicious actors will; if the security of common systems is breached in the future as a result of this Act, it is possible that ordinary Australians will be disproportionately affected.

Given the discovery of significant security vulnerabilities in the past year that can affect most of the devices used by Australians (eg. Meltdown [5], Spectre, KRACK [6] and BlueBorne [7]), it has become apparent that the government should move to increase its security posture by working to fix vulnerabilities; however, the actions enabled by the Act perform the opposite function and may compromise the security of Australian devices into the future.

Minister, I leave you with one final thought: the Act provides little judicial oversight to the surveillance of citizens in the name of national security. Currently the only nations with this power are autocracies such as China; do you suggest we should follow their poor example?

Thank you

[1] - The Guardian - 'AFP data breach: six cases of alleged police misconduct investigated ' - 29 Apr 17 - <https://www.theguardian.com/australia-news/2017/apr/29/public-metadata-six-cases-of-alleged-police-misconduct-investigated>
[2] - Android Open Source Program - 'About the Android Open Source Project' - <https://source.android.com/>
[3] - OpenPGP - <https://www.openpgp.org/>
[4] - Open Whisper Systems - 'Is it private? Can I trust it?' - <https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it-?
[5] - Kocher, P et al - 'Meltdown' - Graz University of Technology - 04 Jan 18 - <https://meltdownattack.com/meltdown.pdf>
[6] - Vanhoef, M & Piessens, F - 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2' - KU Leuven - 03 Nov 17 - <https://papers.mathyvanhoef.com/ccs2017.pdf>
[7] - Seri, B & Vishnepolsky, G - 'BlueBorne' - Armis Labs - 02 Dec 17 - <http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf?t=1536082501386>

Aaron Turrill
[redacted]