Submission related to the proposed 'The Assistance and Access Bill 2018'.

I have several points to make, and as such I will note them seperately.

I would first, however, like to point out the ludicrously short amount of time allowed for submissions to such a wide-ranging attack on the privacy of Australians (and by extention those of the UK, USA, NZ, and Canada).

1. Insecurity: There is no 'middle ground' when it comes to device security; it is either secure or it is not. If the device is insecure to the Government then it is also insecure to other operatives. No software is perfect and deliberately creating a backdoor into a system will certainly also create other avenues of attack. With every Australian device compromised you can be sure that criminal organisations and State actors will be working hard to find and exploit any inecurities. With over 25 million mobile devices in Australia, plus the ubiquity of PCs, gaming consoles, and Smart TV's, any flaws (and there *will* be flaws) in the system will be hugely magnified. Backdoors are not just for 'the good guys'.

2. Oversight: A Technical Assistance Request is voluntary, and is not included in the Annual Report. Even the targets of a TAR are not required to disclose it to their users.

3. Accountability: This goes back to point 2; if there is no oversight, there is no accountability. There is nothing, ultimately, stopping an authorised person from persuing a personal or political vendetta against a reporter, against a class of people (see RoboDebt, see also the government doxxing people who complained about RoboDebt), or against a former partner (see Police accessing personal details of former partners or former partners of associates) if there is no public record of the access requests.

4. Individuals vs companies: The legislation covers an individual if *"…the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end users in Australia"*, which looks to cover every piece of software, or mobile app, that connects to internet or produces content that is going to be used on the internet. The justification for the scope of this category is not clear. As the legislation will be applicable to both individuals and companies, there is need for clarification as to whether an employee could be the subject of a notice or request as a result of their job. What safeguards are there for both the company and the individual?

5. Scope Creep: Legislation almost never narrows its focus, but rather expands it. If the proposed legislation existed several years ago, it could have been used in the RoboDebt debacle, potentially with no disclosure. There appear to be no safeguards in place to prevent (or at least limit and delay) such Scope Creep in the future.

6. Punitive: The proposed legislation provides for ten (10) years jail for 'whistleblowers', with no Public Interest Test. Whilst there are arguments for keeping secret active investigations, such effectively limitless and punitive secrecy goes against the principals of open democracy.

7. Avoidance: We have already seen terrorist organisation adapting to the 'new reality' of pervasive surveilance by 'going dark'. What is to stop the stated targets of this legislation avoiding backdoors

by creating their own devices such as a roll-your-own Android system and rendering the legislation toothless? Alternatively, one could simply purchase a device from the United States, where the First Amendment, via the compelled speech doctrine, prevents the Government from forcing anyone to do virtually anything, including implementing backdoors (see Code is Free Speech). As the use of encryption tools is quickly becoming a skill for criminals (and this use is one of the stated reason for the need for this legislation), eventually the only people who would still use tools subject to the government mandate will be the dumb, low-level criminals and ordinary people without the knowledge or incentives to adopt other tools, and the repercussions of weaker security for those people could be serious and long-felt.

8. Similarly to point 7, if the Government required Huawei (for example) to provide a backdoor into their devices, in theory the Chinese Government will also then have access.

9. Availability: If a company does not wish to comply with a TAN or TAC, they can simply withdraw operations from Australia. It will be hard for the Australian Government to impose the proposed Bill onto a company or individual with no ties to Australia. Further, the requirement for backdoor access does not differentiate from an international corporation and an individual and the ability of each to comply.

10. International repurcussions: When the 'enlightened West' considers legislation such as this, as it has been doing on and off for a generation or more, it provides further cover for less open nation-states to do the same. The Chinese Government already has laws compelling access. Saudia Arabia would no doubt love to compel Grindr to provide user details The oligarchic police state known as Russia has banned Tor.

Ultimately this legislation should be shredded and never spoken of again, but if it is kept it *must* be improved from its current nebulous state. Suggestions include:

- Technical Assistance Requests should be included in the annual report;
- Recipients of notices or requests should be mandated to provide transparency reports, including all requests and notices, broken down by agency, and wether or not the request or notice was complied with;
- Abandonment of both the Technical Assistance Notice and the Technical Capability Notice;
- Technical Assistance Requests should be covered by the same limitations as described in Division 7, namely they should not be able to request systemic weaknesses, nor develop new techniques for removing electronic protection;
- The scope of the legislation should be restricted to only the most serious of crimes or threats to national security;
- Clarity must be provided as to those who breach the legislation unknowingly (317ZA(2);
- Clarity must be provided on the delivery of notices to a employee of a company vs the company itself;
- Clarity must be provided on what is an is not a Communications Provider;
- Upon completion of a line of inquiry, or after a mandated time after the beginning of an enquiry,

or at the culmination of a legal case, whichever is sooner, disclose all aspects of the line of enquiry including but not limited to the devices, software, and target(s);

- A Public Interest Test to determine whether the unauthorised release of information was warranted (as of the draft there is a penalty of ten (10) years jail irrespective of if the release is in the public interest;
- Regular, open audits;

Certainly there are times when interception is necessary for national security, and there is always going to need to be a balance between privacy, transparency, and security. All three of those concepts are important, however, and security cannot be assumed to automatically trumps all other values. Whilst we should work to prevent such attacks on our security and society, we cannot sacrifice the same freedoms that are under threat; to do so would hand a victory to our opponents. This is the very definition of winning the battle but losing the war.

I urge the Government to reconsider the proposed legislation.

Michael Van Boeckel