From: Benjamin Dobell
To: Assistance Bill Consultation
Subject: Opposing the Assistance and Access Bill 2018
Date: Monday, 10 September 2018 12:00:36 AM

Dear Sir/Madam,

I'm very busy, so will keep this brief.

I'm writing to you in a personal capacity, but would like to make it known that I have extensive relevant technical knowledge, as I am a software engineer, Director, and the Chief Technology Officer, across several different companies in technology space. I have extensive knowledge regarding utilisation of encryption and user privacy.

Quite frankly, the Assistance and Access Bill, as it stands, is a complete and utter farce. It is completely inept in its abilities to achieve its *purported* goals. Nonetheless, either as a result of intentional abuse of power, or just egregious incompetence, is entirely over-reaching in its erosion of civil liberties of the Australian people. The act is anything but proportionate, and I can with absolute confidence state that anyone, whom claims to understand the relevant domain, and yet thinks otherwise is either moronic or malevolent.

The use of scare tactics that are being utilised in order to try push this bill forward are utterly despicable and those involved should be ashamed of their actions. We already have in place a fantastic (court overseen) system, that works fantastically well for all the cases that are truly in the public's interest.

As an example, I shall refer you to comments made online, October 5th by Managing Director of Aussie Broadband, Phil Britt[1]:

> tonight l received an urgent call from law enforcement for a person that was in imminent danger of self harm and had been chatting on a beyond blue style website. I was provided with a warrant via email and due to static IP l was very quickly able to provide the end users details to have an ambulance and police dispatched. This is a positive example in my view of what can be achieved when Telcos and law enforcement work together.

This quote demonstrates not just how effective or existing system is, but also how *efficient* it is. Evidence was presented to a court, a warrant granted, served and acted upon, including dispatch of an ambulance in what was clearly a very short time-frame. If a member of a Government organisation or officer of the law is claiming that they're having difficulties obtaining warrants, or that the procedure is cumbersome, then they're either lying or attempting to abuse the system, and our judge's are rightly stopping them from doing so.

Firstly, warrants can already be served if the Government wants to place a wire-tapping order. Secondly, this act is ineffective, as it's quite literally impossible to prevent malicious actors from communicating securely using end-to-end encryption. Why? Because end-to-end encryption is implemented on either end of the connection by the users, it *cannot* be decrypted by anyone else. Forcing companies to disable (or provide a back-door) for services they operate is pointless; malicious users will simply not use third-party provided services and instead use their own end-to-end encryption; which is entirely trivial for any sufficiently motivated persons to achieve. This will not stop terrorists, and it

won’t stop anyone who commits crimes systematically, sex offenders and alike. It will only be useful in catching the most “simple” criminals e.g. the severely mentally disturbed, whom are already trivial to catch.

Instead, all this bill does is erode Australians right to privacy, self expression and political freedom. The act also completely removes the right for Australians working in the tech sector to behave ethically. Instead, this act allows law enforcement to force tech works to behave unambiguously in an immoral fashion, and punishes tech workers who do not comply with fines, and sends those who speak-up to jail. In fact, it’s even more over-reaching than simply tech workers, as practically all businesses operating in this day and age are assisted by technology in their interaction with customers/clients.

When I say that the bill erodes Australians right to self expression and political freedom, do not be confused and think otherwise. This isn’t an accident of wording in the bill, but rather a very clean and intentional goal of the bill as pushed by spy agencies operated by members of the Five Eyes intelligence alliance. As evidence to the fact, I refer you to a quote from your very own website[1]:

> We are also increasingly seeing the use of online spaces to spread disinformation, sow division, and undermine our democratic institutions. The proliferation of interference activities and disinformation undermines the trust of citizens in online communications and information, delegitimizing the benefits and opportunities that communications and social media platforms create.

Now, who exactly will be responsible for deciding whether someone is spreading disinformation, sowing division or undermine our democratic institutions?

It certainly won’t be the Australian public, won’t be juries, or the courts of Australia. This bill strips that right away from citizens and our legal system, instead these *judgements* will be left to some of the most secretive organisation in the world; those who operate in shadow without public scrutiny and without supervision by our legal systems. This bill is *designed* to utilised against those in opposition of the Government. In a democratic society this is an utterly unacceptable compromise to make. This fact alone ought to be enough to see this bill, or any bill even remotely resembling it, struck down indefinitely.

Regards,
Benjamin Dobell

[1] Phil Britt re warrants - https://forums.whirlpool.net.au/archive/2644933#r57303871
[2] Five Eyes statement - https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/countering-illicit-use-online-spaces