From: Matthew Davis
To: Assistance Bill Consultation
Subject: Submission to consultation on the Assistance and Access Bill 2018
Date: Monday, 10 September 2018 12:43:21 PM

Dear Minister

I write to express grave concerns over the dangerous draft legislation titled 'The Assistance and Access Bill 2018'. I am writing both as a citizen who consumes technology, and also as a developer who creates and operates websites, apps, bots and other software.

This bill is a harmful attack on the encryption required for citizens and companies to live and operate safely and securely. The existing warrant powers for law enforcement are sufficient.

1. This bill contradicts itself. Claims that this bill will not force providers to create backdoors are proven false by other sections of the bill itself. The overly vague term "acts and things" is defined in the bill as "removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider". That is, the government will force providers to create backdoors. The term "systematic weaknesses" is not defined. For example, under this legislation I may be asked to capture the secret credentials of a user on the client device, prior to encrypting data. Such an act would not involve changing the encryption algorithm, or breaking the end-to-end encryption to decrypt at a midpoint teel. So there would be no "systematic weakness". But it would nonetheless be a backdoor.
2. As a website and app operator, I strongly disapprove of the possibility that the government can force me to do something technically difficult and expensive, forcing me to pay in time and money. Under the legislation I will have to pay any "reasonable" financial cost. "Reasonable" is not defined, and it's not clear how easily I can challenge that. The legislation does not seem to consider the timeline of the events. For example, I may be served a notice which costs $1M to implement. Under this legislation I will be forced to pay out of my own pocket immediately, and then if I'm lucky, under the undocumented process I may get the government to pay me back eventually. In the meantime my personal finances or the company may be cripled. Similarly, if a notice requires many man-hours, it would be a significant burden on a small startup company to comply. This is harmful for our economy. The writers of this bill seem to be unaware of how challenging it is to install malware, buggy-black boxes, wiretaps etc on securely architected systems. The government should be forced to pay for all the costs incurred by their notices.
3. The scope of this bill is ridiculously broad and unnecessary, where it mentions "protecting the public revenue" and "economic wellbeing". The motivations for notices being served include cases which are not in the interest of a democratic nation. "protecting the public revenue" is prone to abuse because it is too loosely defined. This means that notices can be served to track and attack innocent citizens who are raising awareness about illegal operations commited by Australian corporations. Whenever someone tweets about how the Adani Coal mine dredging will kill the Great Barrier Reef, that makes the mine less likely to proceed, which means tax revenue is threatened. Similarly, anyone spreading videos of abusive abattoirs is causing economic harm, but for the greater good. A democratic society must not legalise the weaponisation of citizen's own devices and systems against citizens' legal protest. This term should be made for more restricted and specific.
4. The scope of this bill is ridiculously broad and unnecessary, where it mentions "interests of Australia’s foreign relations or the interests". It is undemocratic to spy on and attack citizens to protect the interests of a foreign country.

5. The scope of this bill is ridiculously broad and unnecessary, because it allows notices to be served directly to lowly non-technical employees of a company who don't understand the implications of what they are doing, and it may prohibit them from disclosing what they are doing to their superiors. Forcing disinformation upon a company is bad for the economy, and the ethical wellbeing of our citizens.
6. In the USA, the TSA has a master key for most luggage locks. They promised to keep such privileged access carefully protected. However, through reckless incompetence their media team published photos showing staff holding the master keys. Now the keys are available online as files which can be 3D printed by anyone. Through their recklessness everyone's security has been compromised, and the TSA has not apologized, acknowledged their mistake and the damage it's caused, or attempted to correct the issue. This is what happens when governments try to create the powers like those in this bill. There is no reason to expect that this bill will not lead to the same style of unmitigated disaster.
7. The lack of independent oversight and avenues for appeal is a recipe for disaster. The government claims that there will be sufficient protections. However they made the same claims about metadata retention. Abuses under that scheme happened within 2 weeks of the legislation taking effect.
8. The Home Affairs website cites as justification for these laws a case where a sex offender sent text-only messages remotely to a few people. Installing literal malware on Australian's devices and important systems is a disproportionate step towards preventing a few text-only messages. As an analogy, consider the fight against prostate cancer. If the government legislated mandatory, hourly prostate exams for all Australians, all such cancers would be detected early and treated early, and we would undoubtedly save thousands of lives. But the financial cost and invasion of privacy is simply not worth it. The same is true of this bill.
9. This bill will not achieve what it is supposed to. Lone terrorists (such as the Lindt Cafe gunman) obviously do not communicate plans with anyone else, since they are lone wolves. So there is nothing to capture. The small group of gunmen who attacked Paris in 2015 used unencrypted communications. Large organizations like ISIS - who are willing to murder large groups of innocent people - are not going care about an Australian carriage service law. They'll continue to use communications free from Australia's backdoor powers. To believe otherwise is delusional. If you outlaw security and privacy, only outlaws will have security and privacy.

All technologies can be used for good and evil. This legislation will create great harm for those good users, whilst doing little to stop bad users.

Regards,
Matthew Davis

Matthew Davis
[redacted]