From: Harley Jonelynas
To: Assistance Bill Consultation
Cc: [redacted]
Subject: Assistance and Access Bill 2018
Date: Sunday, 9 September 2018 8:30:13 PM

Dear Sir,

In regards to the Assistance and Access Bill 2018, I strongly believe that not only would the digital security and privacy of law abiding Australians be compromised, but this legislation would fail to adequately provide the outcomes it sets out to achieve. In my professional opinion as a Software Developer, as well as in my personal opinions as an Australian citizen, the potential harm this piece of legislation, in its current form, would bring far outweighs any positives it presents. I do understand the challenges that law enforcement face due to encryption, but however it would seem they are still currently able complete their jobs without such measures proposed within this bill. I believe their efforts should continue to be focused elsewhere rather than attempting to dismantle a core component of the internet, in ways which would cause harm upon more than suspects in criminal cases.

The internet is a key piece of technology in this current age, and encryption is one of the pillars it is built on. Encryption is not just a tool that criminals and terrorists use to conceal messages, but it is the defining piece of the modern internet which provides security, privacy and trust in an otherwise open and public platform. Although the Assistance and Access Bill 2018 claims throughout to not introduce 'backdoors' into encryption itself, what it does do, not only enables, but legally forces the introduction of solutions which have the same effects and with it the same behaviours. This is my first objective to this bill. It is both misleading and disingenuous for it to claim there will be no backdoors and that requests do not require 'systematic weaknesses' to be introduced. These are clearly backdoors, perhaps not in the encryption algorithms themselves, but in the software and devices which utilise them. I believe no bill which deliberately intends to confuse and confound the Australian public should be supported, and would hope my representative in parliament would agree on such a principle.

My second issue with this bill is the lack of transparency. Although involuntary assistance requests will be included in the Minister's annual reporting, requests which have been met voluntary are not. There is no valid reason, in which I am aware, why such requests should be excluded from such reports, and believe that this may be intended to allow government and law enforcement agencies to conceal behaviour which may otherwise fall under public scutiny. This is a major concern to me, and I'm sure many others. How can the Australian public be expected to trust that governments and the various agencies conduct their business with integrity, and for the good of the nation when it's activities are hidden away like those of the shady criminals it claims to protect us from. Even worse is the penalties for any individual which exposes potentially corrupt, morally wrong, or other behaviour which acts against the public interest. This is my third issue with the current state of this bill. While I understand the need for confidentiality during investigations, it is important that this is not overly extended with the intent, whether deliberate or coincidental, to prevent not only the public, but elected governments and potentially courts from being able to assess the quality of law enforcement practices and the laws surrounding them.

I claimed above that I do not believe this bill would achieve what it sets out to do in

regards to collecting evidence to be used to prosecute terrorists, paedophiles, criminal gangs, or whatever emotive buzz words are chosen to sway public opinion of the day. Simply put, the measures put in place, if this bill would indeed become legislation, would only be able to compromise law abiding citizens and those criminals who have not put even the slightest thought into protecting themselves from law enforcement agencies.
It could easily be bypassed by self-hosting or using services outside the jurisdiction of the Australian government, their allies and cooperating parties, as it requires intervention by the provider of the services in one way or another.
This brings me to one of the more laughable issues I have with this bill. The requirement of foreign providers to also be subject to such requests and face the same punishments from refusing to comply. I highly doubt this would work in countries which criminals would choose to base their communication et al services to avoid law enforcement, especially when the government already has issues enforcing even basic tax laws for companies 'based' overseas.

The scariest part of this bill is not what it enables our law enforcement agencies to access, but what it allows third parties to through the introduction of "not backdoors" (but really backdoors) in critical software, even beyond messaging applications. The thing about encryption and software vulnerabilities is that adding a entrance (which may or may not be at the back), even with a lock on it doesn't prevent someone else from using it. In the physical world a criminal can only be in one place at a time and to break through a lock requires them to spend time there and not elsewhere. In the digital world they can be in many places at once, breaking as many locks as they want. These holes that will inevitably be added, even though they may be requested to be used against a specific target would most likely be developed in a way which would allow them to be used against any user of a system. It would be logical to do so from a software development perspective, as it grants the ability to comply with future notices without additional development resources and costs. The looming danger of such solutions is obvious, a new way for hackers both domestic and foreign, private or state sponsored to compromise security and retrieve your data unauthorised. As the Internet of Things (IoT) continues to grow, these might not just be emails and messages, but could include all sorts of appliances and even medical equipment.

In summary, my issues with this bill are:

- It does not provide adequate safeguards for law abiding citizens to ensure their data is protected
- It compromises the security of potentially all devices connected to the internet, which continues to grow everyday
- The punishments for non-compliance or even reporting on requests are not 'reasonable and proportionate' as the bill claims
- It conceals the conduct and erodes the public trust of law enforcement through, at times, clearly unnecessary secrecy
- It encourages developers to add backdoors and systematic vulnerabilities to avoid unreasonable and disproportionate punishments, which would unintentionally allow third parties (including foreign governments) to exploit and gain unauthorised access to critical data belonging to Australians
- It is currently written in a matter which is intentionally misleading to the public through its claim of no 'backdoors'
- It erodes the trust in important infrastructure currently protected by encryption and similar technologies such as banking
- It is easily circumvented by criminals, and as such merely compromises the digital privacy and security of the general public
- There is no legal requirement for reporting voluntary requests currently written into

the bill

Yours faithfully,
Harley Jonelynas