Assistance And Access Bill 2018

Thank you for the opportunity to make a submission on the proposed **Assistance and Access Bill 2018** (https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018). Given that these measures have been proposed in public for many years, a public consultation period of four weeks is woefully inadequate, and serves only to prevent thoughtful and complete analysis of the content. As such, this submission is limited to only a small fraction of the overall bill.

In summary, it seems that this bill is fundamentally designed to implement state-access backdoors in the communications systems we rely on. The protections and oversight in this bill regarding “systemic” weaknesses and “voluntary” vs “compulsory” orders are not fit for purpose, and if implemented would serve only to undermine the trust and reliability of systems, as well as damaging Australia’s economic and security interests.

The lack of any legislation protecting fundamental human rights such as free speech and free association means that this bill would be able to effectively compel Australians to passively deceive or actively lie, potentially destroying professional careers without achieving the goals the bill intends.

Systemic Weaknesses

Section 317ZG appears to be drafted as a defense against the claims of undermining the trust in existing encryption systems. However, there are two key problems with this section which mean that these defenses are not only worthless but actively counterproductive.

“Electronic Protection”

The term “Electronic Protection” is not defined anywhere in the bill. It seems from the explanatory document that the intent is to narrowly draft this term to refer specifically to “encryption or authentication mechanisms”, ie: limiting its scope to prevent the “war on maths” style backdooring of pure algorithms.

However, security and trust in any encrypted system relies on viewing the communications system holistically. All communications software is built and structured in layers. The simplest model, OSI (https://en.wikipedia.org/wiki/OSI_model) has been in use since the 1970s, and a published standard since 1984. Of particular note is that the OSI model explicitly includes everything from the Application layer (for example, the keyboard and rendering layer in Facebook Messenger) down to the Physical communications layer (for example, a piece of copper wire, or a radio wave). This model covers the entire system, and the design of any trustworthy system must be done in the same manner. In modern systems, almost every one of these layers even down to the forming and reading of radio waves themselves is implemented in software.

A weakness at any layer is, by definition, a systemic weakness. A protection at any layer is, by definition, an electronic protection. Entirely bypassing the protections of any layer, as described in the explanatory document ("a notice may require a provider to facilitate access to information prior to or after an encryption method is employed, as this does not weaken the encryption itself") is by definition, a systemic weakness in electronic protection.

Fundamentally, any system is only as strong as its weakest link. This bill might be intended to prevent weakening the strongest link of encryption, but only by removing it from the chain entirely. Any reasonable interpretation of the word "systemic" has to consider the effect on the whole chain, not merely the encryption link.

At a minimum, the bill must be redrafted to ensure that the test described in the explanatory document matches the legislation, applying the "degree to which malicious actors are able to exploit the changes required" test described there to the entire system rather than limiting it to "electronic protections".

"An offer you can't refuse"

While the bill contains clauses intended to prevent backdoors in encryption using Technical Assistance Notices (TAN, compulsory) or Technical Capability Notices (TCN, compulsory), nothing prevents them from doing so using Technical Assistance Requests (TAR, voluntary).

These voluntary requests have virtually no oversight, are not included in Ministerial reports, cannot be publicly disclosed or discussed (S317ZF) and are not constrained by the powers in the act which purport to prevent encryption backdoors (S371ZG).

There is also nothing preventing the threat of TAN or TCNs from being used to defacto require backdoors under TARs. In effect "Either backdoor this encryption now (TAR), or spend the next year rebuilding your system to our design (TCN)". Truly for any business in 2018 this would be "an offer you can't refuse"

At a minimum, the bill must be redrafted to ensure that TARs have the same limitations, review and oversight as TANs and TCNs.

Open Source Developers

S317C of the bill is incredibly broad, and is drafted to apply to virtually any person with even the most tenuous connection to Australia. A parent who installs ABC iView for their family to watch is a communications provider. A child of 5 who's online game downloads the latest update is a communications provider. Even without these edge cases, hundreds of thousands of Australian open source developers are now communications providers who this bill would compel to make changes and actively lie about it.

Open Source

Open source development underpins the modern internet. Every part of the systems Australians rely on for their daily life, interacting with government, businesses and each other runs on open source software. It is beyond the scope of this submission to describe open source, but fundamental to the flaws in this bill is the fact that open source development is done in the open, with code, designs, reasoning, and documentation done in full view.

This is not a mistake or misdrafting, popular open source messaging systems such as Signal and Mastodon are clearly meant to be covered by this bill as are the administrators of forums, chatrooms or similar.

S317E(1)(j) compels people to "conceal the fact that any thing has been done", while S317E(2) attempts to prevent people being compelled to deceive or make a false or misleading statement about a change. However, this clause is incredibly narrowly drafted and only offers protection on the change itself, offering no protection to developers forced to lie and deceive about the **reasons** for the act. If an open source developer receives a Technical Assistance Notice (TAN, compulsory), Technical Capability Notice (TCN, compulsory), or Technical Assistance Request (TAR, voluntary) then they are compelled under 317ZF not to disclose even the existence or non-existence of any such request or notice except under very limited circumstances

The incredibly limited circumstances 317ZF allows for a developer to even discuss the notice are also an antithesis to open source. A developer receiving such a notice is only able to seek legal advice, not the technical or peer advice which underpins virtually every other collaboration in open source development. Balancing this tightrope will require specialist legal advice, something most open source developers will not have access to without financial hardship, and practically means that the supposed protections provided by S317E(2) will be moot.

At a minimum, this bill must be redrafted to ensure that the protections in S317E(2) extend to the disclosure of a request or notice under 317ZF.

Professional Suicide

Open source development largely proceeds by "forking" existing systems in order to add new or complementary features. It is beyond the scope of this submission to describe this process in open source, but a reasonable summary might be that where an existing system is perceived to have a weakness or lack a feature, other developers are encouraged to take the existing system and build a new system base upon the old. This process of "standing on the shoulders of giants" drives the evolution and creation of new systems.

Open source developers also take professional pride in their work. For many, their open source contributions are their valued professional resume and are critically relied upon in many cases as proof of both their ability and ethics. Under this bill, requiring a developer to

weaken an existing system and actively lie about their reasons for doing so would be forcing that developer to effectively destroy their professional body of work, actively damaging their career and by extension Australia's productivity.

In most cases, the change would be discovered and the developer quizzed. Even for a developer caught in this Catch-22 situation trying their absolute best to walk the disclosure tightrope this this bill requires of them, the existence of government notices/requests would be quickly inferred or assumed. At this point, other developers in global jurisdictions not covered by this bill could trivially reverse the change, or fork the project - rendering the entire change worthless and leaving only the wreckage of a professional career.

This bill as written will damage Australian open source developers worldwide, damage their professional standing and hurt Australia's information technology sector irrevocably.

At a minimum, this bill must provide developers a way to challenge or refuse a request when the development process (such as open source) would render the change trivially discovered or inferred. The complete loss of a developer's intellectual property and reputation due to no fault of their own must be prevented.

Summary

By requiring that covert backdoors be implemented in the systems they rely on daily, this bill will cause naive consumers will have their protections weakened and their online lives made vulnerable while informed consumers will simply avoid or replace those systems. By using the voluntary request powers under this bill under the threat of coercive compliance notices, covert backdoors can be forced into any part of any system. By requiring that developers actively lie to conceal the existence of both requests and notices, this bill coerces developers into speech or silence, robbing them of one of their most fundamental human rights. By trapping open source developers in a catch-22 of compliance and silence, this bill will destroy careers without in any way achieving its goals.

This bill will not only fail to work in the way it's intended, it will actively harm Australia's economic and security interests.