Submission to Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Ross Paine

07 September, 2018

I'm writing in response to the exposure draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 I wish to indicate that I **oppose** the Bill for the following reasons;

1 It's unworkable

The scope of a 'designated communications provider' extends all the way to any singular person that provides software in connection with an electronic service that has an end user in Australia.

As a person that that would encompass I can confidently say, that I am not equipped to be carrying out counter terrorism activities on behalf of the government.

2 Increased risk

Software security is hard, it takes extraordinary attention to detail and effort to minimise attack surface and to ensure that vulnerabilities are not introduced into even the most trivial of software.

By requiring that software be modified for third party access, even if not requiring the creation of a 'systemic weakness', you're introducing a massive attack surface for other malicious third parties to exploit. Add the situational pressure that would inevitably come with having a federal agency demand that assistance be rendered multiplies the above risk.

This doesn't seem to be of concern to the Department, they have not, to my knowledge consulted with anyone outside of large businesses, but it should not be underestimated. You may find that the legislation will interact with regular people that will not have the legal expertise to understand their requirements under the proposed changes, nor might they have any experience in offensive cyber operations, which is essentially what they will be asked to assist with.

3 Counter productive

It must be understood that secure software evolves in the face of a threat, that's it's nature, the mentality of a software author, when they are trying to write secure software is to understand what their threat surface is and to mitigate against it.

Additional legislation that immediately presents a hypothetical new threat surface will be countered by new software that would render the legislation meaningless.

4 It won't work

If the software is well designed, it should not be possible for a third party (including the original author) to alter the code on the users device, and if the software in question is true end to end encryption with perfect forward secrecy (PFS) it should not be possible to provide access to a third party.

In the case of open source software there is a further complication, because the changes that enable the vulnerability would be published in source code, visible to anyone that cared to look.

5 It's unclear what could be required

It's not clear that the 'systemic weakness' exclusion is broad enough to prevent an agency from compelling a provider to disable specific security functionality.

As an example, one might argue that it's 'good enough' to have encryption without PFS, whether it is or not, it's highly unlikely that every 'designated communications provider' would have the resources to argue with federal government agencies if they decided that was the case.

It seems obvious that disabling an effective PFS system would be high on the list of priorities for a security agency, because when coupled with the power to sieze property

(and thus easily compromise the private key) it would enable the reading of archived messages.

It must be made clear what the extent of a 'systemic weakness' is, does it exempt any softening of any system, or does it allow softening down to some arbitrary baseline level?

6 It will harm the industry

Software must be one of the most globalized industries in existence, if the burden of implementing the kinds of vulnerabilities proposed by the Bill is placed on the industry in Australia, it will result in moving operations for any software development that takes security seriously off-shore. In the process you limit the employment opportunities for software developers in one of the most critical modern fields, cyber security. Given the legislation that's proposed, one has to imagine that the Government is already struggling to attract talent, it defies belief that they'd take further action to erode the industry.