As the Commonwealth mentions in the explanatory document,

> “Encryption enables Australians to confidently engage in activities online such as banking, shopping, communications and other services”

Backdoors.

Cryptology makes it very difficult for a third-party to access data. The Commonwealths enforcement of a mechanism whereby it can request access to the encrypted information means simply that a mechanism must be produced that allows decryption by a third-party.

This can be either by the supplier of the product resulting in multiple requests to a the owner. This approach would not seem to be timely for criteria use.

Or the supply of a tool allowing third-parties to access this information. Once it is known that a mechanism of any sort exists that will bypass encryption, other third-party players will seek out this mechanism. Whether a disgruntled employee leaks it to the world, such as the leak of the NSA toolset, or security experts will attempt to duplicate the tool, for example the recently discovered God Mode bit found in Intel CPU’s. Intel CPU’s are used in the majority of the desktop computers. The “God Mode” allows desktop security mechanisms to be bypassed.

So what is the problem?

Australia has a very good record against terrorism. The only known successfully cases of “terrorism” seem to involve single actors committing crimes. In my opinion, these single actors seem to have mental disorders which triggered their actions rather then just terrorism.

If a smart criminal wishes to hide communication and/or data from the authorities, it is possible for him in his own right to implement an data encoding system independently of any third-party products.

One example used to justify access is that the Victorian police allowed somebody “to get away” because the police could not access his phone. This, as a justification for widespread access to secure device, seems incredulous. How could somebody “get away from” from police custody if there was sufficient evidence to hold him. The implication is that he physically escaped which has nothing to do with decrypting his phone.

Overreach and bypassing the judiciary.

Using the same example the question then needs to be asked, how did he gain the attention of the police? Was there sufficient evidence for a judge to consider that there was the likely hood of a criminal act have taken place. If there was then why wasn’t a court order issued for the accused to hand over access. If the accused then refused surely he would have been in contempt of court and thus held till he complied.

So using this dubious example seems to be more a reason for justifying the removal of judicial oversight rather the finding the truth of the matter.

Bypassing the judiciary in it own way is as disastrous as providing mechanisms for breaking encryption. The “secret” FISA courts in America, while a judicial court, it was a court of secrecy and thus limited scope for having oversight. This has resulted in the FBI using fraudulent documents to obtain warrants to spy on the Trump. Just imagine how easy it would be to initiate a similar action, if there is no judicial oversight. A perfect example of why no judicial oversight is such a bad idea.

Impact on Industry

As in OSIA’s arguments against the TPP-11, insufficient thought has gone into the ramifications of the implementation of this legislation. The potential impact on copyright as outlined in OSIA submission to the senate attempts to overwrite international copyright laws with a requirement that suggests that software released under an Open Source software licence need not be followed.

If implemented the copyright provisions in the TPP-11 has this has the likely hood that open source software will migrate to a state outside the TPP in order to ensure international copyright laws will be upheld. This possibility is only going to be reinforced under the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.

> *“…the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one or more end users in Australia”*

This single statement alone has significant impact on the software industry. Any person that supplies software “likely to be used” anywhere in Australia or its territories in now subject to Australian Law. Let that sink in! Australia is claiming jurisdiction over non-Australian citizens. Foreign citizens to foreign companies and the foreign companies themselves, with no legal standing under Australian law, would be bound under Australian Law. It is easy to say that if these same foreign companies wish to sell products in Australia then they must obey Australian Law but in reality what is likely to happen to what is predominately a small world market.

- The foreign companies decide not to supply their products to Australia as the potential costs outweigh and potential profits.

- A separate Australia only product is produced that has flaws, refer above.

- A TPP-11 country mounts a ISDS challenge to the laws.

- A foreign state lodges a complaint with the WTO.

- And so on…..

Following on from this, there a number of issues under this legislation that concerns me greatly.

The affect on me personally.

In order to not be held personally responsible for the provisions under this legislation I can see further immigration of skilled workers to other countries. As with the TPP-11 legislations attempt to overwrite international copyright laws, we now have potential legislation that would hold me personally responsible, as an open source developer, for any use of my source by third-parties.

In order to limit my exposure to this legislation, I would need to immigrate and thus change my citizenship, thus depriving the Commonwealth of a taxable income. This does assume that Australia is not going to assume jurisdiction outside it;s own territory or citizens.

I could stop producing software altogether thus depriving the Commonwealth of a taxable income. I would though have to find an alternate income source.

I could also change the licence terms of any of my Open Source code. I could include a clause that specifically denies permission for my software to be used in any products accessible by the Commonwealth and or it’s Territories. Australia, the only country in the world that has a specific clause in an open source license prohibiting it’s use in that specific country.

So while I’m a minor player in Open Source Software services I would like to point out a few facts regarding the size of Open Source Software industy. Both this bill and the TPP are putting at risk Open Source software development in Australia. This is no small market. For Example:

- Android phone market share is over 80% of the total smart phone market. Android is running on Linux an Open Source operating system.

- Web servers, the infrastructure behind websites has over 85% of the market share, split between two types of open source webservers, NGINX and Apache.

- Open Source based embedded devices is over 75% of the total market. These are devices such as network modems, TV’s, media centres, GPS units etc. Some of which are fundamental devices used within our society. The value of the embedded devices market is expected to reach US$233.19 bn by the end of 2021.

- Of the top 500 super computers in the world, over 99% are Linux based, an open source operating system.

- The Commonwealth websites are based on the Drupal, an open source content management system.

The overall Open Source Industry as a whole is very large.

Two further points I wish make are:

1) Reading this legislation suggest to me that the Commonwealth is attempting to implement legislation for a problem that either does not exist, may be dealt with in other existing ways or with minor tweaks to existing legislation. The breadth of this legislation suggest to me that Commonwealth is attempting to overreach into areas which it should not ,the least being the imposition of law to degrade the security of transactions leading leading to a deterioration of fundamental levels of trust. This view is further reinforced by the secrecy provisions and the lack of judicial oversight that is also proposed.

I am very much against this legislation due to the implications above.

2) The second point I would like to make is that it is becoming apparent that the Commonwealth does not have sufficient expertise in its understanding of the ramifications of it’s legislation has on industry. Both the TPP-11 and this legislation show a lack of understanding of not only the technical

aspects resulting from legislation but a lack of understanding in the societal ramifications of these same pieces of legislations.

I would to propose that if the Commonwealth government continues to refuse to involve industry leaders in drafting legislation then it at least embodies a review body to critique the legislation in its entirety looking at some form of possible scenario analysis.

Mark Phillips
[redacted].