18/12/2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

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

Dear Secretary,

Thank you for the opportunity to make a submission to this inquiry.

My name is Jake Bloom, and I am a software engineer from Sydney. For the past two years I have worked at Facebook Inc (owner of WhatsApp) in California, and starting in the new year I will be joining a health-tech startup that uses encryption to protect patient data. When it comes to the practical implementation of this legislation, I am as close to the coal-face as you could possibly get.

I have ideological, economic and practical concerns with these laws, which I will outline below. I also submit a set of recommendations that I encourage you to adopt.

Ideological Concerns
Personally, I believe that in a democracy, it is important for there to be methods of communication among citizens that is free of government oversight. A good example of the effectiveness of these encrypted communications is the Arab Spring uprisings that occurred starting in 2011, real democratic, grassroots movements enabled by communication free of government oversight.

While I do not seek to compare the Australian Government to the totalitarian Governments of Egypt and Libya before 2011, I believe it is still important to preserve the right of citizens to communicate freely, which this legislation erodes.

While it is possible for other Australians to disagree with me on an ideological point, I wanted this to be known to the committee. My Economic and Practical concerns with the legislation is motivated more by fact and less by belief.

Economic Concerns
Earlier this year, the Australian Government banned Huawei from building Australia's 5G communications network, due to concerns that the Chinese Government may be intercepting traffic. This legislation ensures that there is no doubt when it comes to Australian Technology - the Australian Government is listening, and the public debate around these laws means that the international community has noticed.

For a concrete example, Apple and NASA use Atlassian's product "BitBucket" to store their source code. As a result of the passage of the bill, Apple and NASA know that a capability to read their source code could be installed into BitBucket without notice. As a result, international firms will move away from using Australian made software to power their business, in a huge blow to the Australian export market.

More alarming, however, is that there is currently no clarity as to whether a Technical Capability Notice can be served to a company or an individual, meaning that software companies such as 1Password have already started discussing the future of Australian employees at their company.

In May 2018, the European Union's General Data Protection Regulation (GDPR) law came into effect, which requires immediate disclosure of improper uses of user data (such as turning said data over to the government), no matter how many or few users of the service were impacted. This means that an Australian company that has been subjected to a Technical Assistance Notice or a Technical Capability Notice cannot comply with the GDPR laws and cannot legally export to Europe.

As a result, this legislation cuts off the export market for Australian software companies, and puts in jeopardy the employment of Australians overseas. There are over three hundred Australians employed at Facebook, and all of them are learning world class skills that many hope to bring back to Australian shores one day. This legislation would cut off this learning pathway for Australians overseas and stymie the knowledge that they bring home with them.

Practical Concerns

As I mentioned in the opening of the submission, as a software developer that deals with encrypted messages, I am well placed to comment regarding the impracticality of the legislation.

Firstly, the phrase "whole class of technology" is not well defined, and as a result, the implications of what constitutes a "systemic vulnerability" is unclear. This makes a real difference when implementing the code to comply with a Technical Capability Notice, and could make the difference between safely intercepting one person's data and opening a backdoor for anybody to get in.

Secondly, it is accepted practice when writing software that before you can deploy your code for users to interact with it, it needs to be reviewed by another person. This renders the confidentiality clauses within the legislation useless, as at least one other person will see that a weakness, vulnerability, spyware or redundant code is being inserted. Upon discovering this, it would be raised immediately to management or leadership of the company, and would likely resolve in an immediate termination of the engineer who executed the Technical Capability Notice.

Having worked at a large multinational company, I can tell you that the rank and file employees as well as the leadership would be more inclined to pull a product from a market altogether rather than compromise the security of the application. Given that Apple has

previously declined to unlock iPhones for the FBI, and Facebook and Google are unwilling to comply with Chinese Government to access a market of over one billion people, I find it difficult to believe that these companies would waste time and money making a product less secure to satisfy a market that they can be successful without.

Finally, for many people, being served with a request or notice under this legislation places them into an entrapment scenario, where ignoring the notice would breach laws in Australia and complying with the notice would breach laws such as Europe's GDPR or the USA's HIPPA. This creates a no win scenario where being served with a notice means fines or gaol time in multiple jurisdictions, regardless of the action taken.

Criminal Concerns

An additional concern is that serving a Technical Capability Notice itself is an illegal act, as it engages an individual in servitude under the definition of the Australian Criminal Code, Section 270.4. The definition is as follows:

> *(1) For the purposes of this Division, servitude is the condition of a person (the victim) who provides labour or services, if, because of the use of coercion, threat or deception:*
>
> *(a) a reasonable person in the position of the victim would not consider himself or herself to be free:*
>
> *(i) to cease providing the labour or services; or*
>
> *(ii) to leave the place or area where the victim provides the labour or services*

Under this definition, if an individual was to be served with a Technical Capability Notice, they would be a victim of servitude, as the Commonwealth is not renumerating the individual for building the capability, the individual is not free to cease building the capability, and is operating under the threat of gaol time. Whilst I do not claim to be a legal expert, in my mind, the concept of a Technical Capability Notice seems at odds with this definition.

Recommendations

My recommendation is to repeal the legislation entirely. Failing that, I recommend the following:

- Remove the concept of a "Technical Capability Notice" as it amounts to nothing more than servitude as I outlined above
- Amend the legislation such that Technical Assistance Requests and Technical Assistance Notices can only be served to a corporation, not an individual
- Narrow the scope of the legislation so that it can only be used in the case of terrorism and child sex offences, not the broad scope that currently exists
- Properly define a "whole class of technology"
- Allow the public to immediately view which companies have been served with Technical Assistance Requests and Technical Assistance Notices