From: Naomi Thompson
To: Assistance Bill Consultation
Subject: Assistance and Access Bill Submission - Naomi Thompson
Date: Monday, 10 September 2018 9:41:22 PM

The Assistance and Access Bill has the right intention behind it but the proposed bill is far from perfect. Absolutely encryption can be a big problem when investigating criminals and criminal behaviour. However that does not mean everyone's right to privacy & security should be sacrificed for the convenience of dealing with a few rotten eggs.

I do think companies should be compelled to help where possible but at the same time, orders to compel companies should be subject to oversight to ensure they're issued where it is necessary and not because it's the easy route. The weakest point in any system is ALWAYS the human element. Scams only succeed because humans fall for them for example. As a result, that means that at any point, law enforcement agencies with access to the powers in this proposed bill could be capable of abusing it.

We have seen countless cases in the past where new powers were issued and they were illegally abused. There are also countless cases in the past where well intentioned and legal actions had horrible consequences. Such as the illegal accessing of metadata by police officers and when ASIC (Australian Securities & Investments Commission) inadvertently blocked 249 999 other harmless websites in their effort to take one fraudulent website offline. In the case of ASIC, it took days to realise the stuff up because a secrecy order was issued. If companies are required to keep what they're doing on behalf of law enforcement agencies silent then how can we identify when errors are made?

We teach our police officers to use "reasonable & proportionate" force when dealing with people. If at any time people feel the use of force was not "reasonable & proportionate" then they can make a complaint which is then investigated. This is a good system which provides oversight of police force to ensure it is fair.
Without judicial oversight then there is no check or balance to ensure that the powers being granted in this bill are deployed in a "reasonable & proportionate" way. It is known that prevention is better than treatment and the saying applies here. It's better to ensure the powers used are "reasonable & proportionate" in the first place than to have to remedy the situation afterwards.
On top of this, with whistleblowers being at risk, there is some question as to whether there would be any remedy afterwards.

When the US proposed allowing ISPs to seller customer internet data, several people began crowd fundraising to purchase the data of several members of the US Congress. Who is to say that a government who is no longer popular with the voters wouldn't have a similar response from voters who work in law enforcement agencies with authorization under this bill? Imagine having a politician's home network or one of their personal devices hacked and justified as "reasonable & proportionate"? Without oversight you can not guarantee that this does not happen.

I also think the broad scope of who this bill includes is woefully flawed. I have several friends overseas who develop software. My reading of this bill suggests it would apply to them if I used their software. This is a terrible outcome as it causes Australian law to apply to non-Australians and exposes it to a legal challenge. It also runs the risk of hurting open source development and general software development. It raises the question as to whether other countries might pass laws to directly counter this proposed bill in the future?

The fact this bill grants the authorization to hack any other computer or system to achieve the target of law enforcement agencies has huge risks associated with it. Not only does it run the risk of causing unintended consequences, it also has the ability to violate other laws such as a breach of privacy because once again the human element is the weakest link.
On top of that, it also encourages people to transfer as much as is possible outside of Australia to make it much harder for their systems to be deemed "necessary" to hack or for them to be compelled to apply. If the organizations transfer the data to the EU then you end up with the GDPR applying among other laws. I distinctly remember the EU ruling parts of the UK IP law were invalid whilst the UK was a member of the EU. I can assume they might make a similar ruling on this bill for anything (people or info) held within their borders too.
That then also opens Australia up to a potential international conflict in our relationships with other countries.

When it comes to some terrorist attacks these days, it's clear that the offenders have instead of going more high tech have gone low tech instead and slipped under the radar. This bill does nothing to handle a criminal who decides to communicate face to face or even via old fashioned letters dropped at specific locations for others to pick up.

The broader rights to collect more information under traditional warrants is a concern because you never know what might be collected and how it might be handled. I remember reading recently about a case of a man coming through the airport and Border Force asked to see his phone, he asked why, they said so they could check it. He asked what information they would be copying and the officer refused to answer him even though he handed his phone over without complaint. Who's to say that a person photos or even intimate photos between a couple won't be captured by the expanded collection powers let alone even more sensitive data?

I also read about a man who worked for NASA in the US who had to have is own employment contract violated by the CBP (Customs & Border Protection) agents over there when they insisted on access to his computer and phone. When he told his work, they had to reissue devices to him + change all his access. What's to say something similar won't happen here with say an employee for one of our electricity companies or even BoM (Bureau of Meteorology)?

The concession that the technical capability notices can not require the implementation of a backdoor and that the notices can not prevent the rectification of systemic weaknesses is a good start. If it did not exist and this bill was in force when WannaCry happened, there could have been a push to keep Australian systems exposed to allow access to law enforcement agencies for example. This is why it is a good thing the technical capabilities notices have been reasonably well defined.

However compelling organizations to help can sometimes be a problem. I remember distinctly a case where Apple was compelled by a court order in the US to make a shooter's phone available to authorities however they were unable to do that as they did not have the decryption code. In a case like that, there is not much they can do and fining a company will not change the reality of the situation.

What I'd like to see happen is:

- Judicial Oversight introduced
- Limitations on who this bill applies to - Less likely to capture overseas people where this bill would be hard to enforce against
- Limitations on when it is deemed an organization is "not complying"
- Limitations on the expansion of what can be collected under existing warrants
- Removal of or at least Limitation on when secrecy orders can be applied
- Limitation of who can apply under this bill to use its powers for their benefit
- Limitation on the devices deemed "ok" to be hacked
- The introduction of further mechanisms that encourage working with companies instead of steam rolling them into complying

A simple way to ensure privacy of Australians while allowing access to data of criminals on networks which employ encryption might be a two-factor access portal whereby the law enforcement agency can enter their own login details and the company can enter their authorization on their end which would allow the agency to search the organizations system with the organization holding the logs of those searches so if they identified unauthorized searches they could then take the evidence to some form of oversight. In this example you could also have orders to compel the organizations to provide the second factor of authorization but it would help account for the human error.
It doesn't get around end-to-end encryption but does allow a central point of access for organizations that are the ones who apply the encryption.

In the case of end-to-end encryption, that would be one of the perfect examples of getting a court order to permit the hacking of a device and the placement of some software that captures messages before they're encrypted and sends them to the law enforcement agency.

Both of these examples attempt to provide solutions that allow for the collection of data while preserving the privacy and security of Australians. You can not have a "good guys only" backdoor through encryption. Two factor Authentication is considered reasonably

secure. It is also considered the best standard of practice for end users. There is no reason why it should not apply to law enforcement to ensure their access is secure. It also has the added advantage of providing a buffer against the weakest element of the system - humans.

In summary, I think this bill is deeply flawed and has many many problems with few redeeming factors. From lack of oversight to overly broad powers including who the bill applies to, what can be collected, rectifications for when things go wrong, who has access to the powers under this bill and what is deemed ok to hack. This bill should be thrown out and sent back to the drawing board.
The technical capabilities notices show promise of good legislation but do not make up for the giant problems the rest of the bill contains.

Australia use to be the leading country when it came to information technology and forward thinking. Let us go back to that time when serious thought and discussion was had instead of the constant need to ram through laws for short-sighted needs.

Naomi Thompson

Concerned Australian Citizen