Comments on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Overall opinion

Everyone in Australia should be very worried about the continuing expansion of powers for enforcement and security agencies to intrude into people's lives – always in the pursuit of a mirage, the mirage of total security. The powers that are being granted are not well restricted, not well defined, lack independent oversight and exhibit almost no transparency.

It is difficult to believe that any MP who would vote for this bill actually understands what powers he or she is granting, such is the abstract and general nature of some of the provisions.

Rank hypocrisy

Recently the Australian Government decided to ban Huawei from participating in the 5G network build on the grounds that

> *The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.*

Source: https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

So the Australian Government responds by proposing a framework by which “vendors are likely to be subject to direction from a foreign government”. The Australian government would be creating a situation identical to the situation it is reacting negatively against.

The Australian government didn't start this war but it is certainly escalating it. This framework can only serve to justify what the Chinese government is alleged to do, and embolden it further, and to encourage other governments to do likewise.

(I take issue with the use of the word “extrajudicial” in the quoted text above. It hardly matters whether the direction is extrajudicial since legislation like this proposed legislation is simply making it legal, rather than extrajudicial. What matters is that the direction by a foreign government is likely to run counter to Australia's interest.)

End game

The end result for, by way of example, a mobile phone manufactured by a certain well-known company is that it comes preconfigured with backdoors for every spy agency and enforcement agency, foreign and domestic. The phone is essentially useless if privacy is required. You should immediately ban it for sale in Australia.

Under the proposed legislation, you can of course direct the company not to insert a backdoor for any foreign government but in that case all you do is create a situation where the company has legal requirements that are impossible to meet. It has conflicting requirements that it *cannot* resolve.

Since you can assume that every government's legislation will have secrecy requirements, the company would be forced to deceive you and forced to withhold information from you – at risk of prosecution.

The end game is a total breakdown in the global trade in technological goods and services, with no doubt negative effects on the global economy and on Australia's economy, and a severe pullback in innovation.

In the burgeoning world of the Internet of Things, you can assume that in the near future just about every device is internet connected and capable of communicating over the internet, and hence within the scope of this legislation. https://en.wikipedia.org/wiki/Internet_of_things

There are a number of obvious loopholes in the legislation. So if I look a few steps ahead, to see what people intent on protecting their privacy will do, and what government will do in response, the world that I see is a very ugly one indeed – closer and closer to totalitarianism, but the mirage of total security still as far away as ever.

Another direction

Rather than being part of the problem, the Australian government could be part of the solution. That would mean:

- abandoning this legislation
- banning the sale of any product or service that is intentionally compromised (after all, any such product or service is clearly not “fit for purpose” and breaches the Australian Consumer Law)
- providing resources and expertise towards identifying products or services that are compromised in this way (in other words, making Australia's technology more secure, not less secure)
- encouraging the development of products and services that are provably free of such backdoors
- encouraging other governments to follow the Australian government's lead

However the government's track record in the recent past suggests that it will not embrace this other direction, so I will take a look at the proposed legislation.

Fake example

The examples provided in government documentation always involve “scary” things like terrorism and paedophilia – whereas the legislation never restricts itself to those matters. If you expect to be taken seriously then you should address the yawning chasm between the legal matters that can be used as justification for issuing a Capability Notice and using a capability - and the serious end of the spectrum that always features in the example.

Likewise, the example implicitly talks about bypassing encryption but the legislation in no way restricts itself to that matter.

I **recommend** that this entire framework be limited to dealing with serious crime. You could, for example, incorporate by reference the definition from the Telecommunications (Interception and Access) Act, section 5D. I recognise that the government is engaging in a slow war regarding what is a 'serious crime', progressively weakening the definition but it could at least make a pretence.

Withdraw product or service

One thing that was not clear to me from the draft legislation is whether a company has the option of withdrawing a product or service from the Australian market rather than being forced to provide a compromised product or service. Particularly if a key feature of the product or service is security, it may be entirely reasonable to do this.

Indeed, in some cases this may be the only legal course of action i.e. where the demand from the Australian government cannot be reconciled with other conflicting demands.

I **recommend** that the legislation be clarified to state explicitly that withdrawing from the Australian market is sufficient to comply with the legal obligations under this legislation.

Dishonest

317E Listed acts or things, clause (2), provides that only in the case of (1)(j) is the company protected from being forced to behave in a dishonest way. Why does that not apply to all items in clause (1)? Putting aside the fact that everything in (1) is inherently dishonest, why not ensure that a company, while complying with the basic intent of this legislation, can never be forced to make false or misleading statements? It is understood that this legislation can force a company into silence. It is a step beyond that to force a company into lying.

I **recommend** that this legislation be enhanced to provide the specific form of words that a company is to use when it is asked a question that it is not permitted to answer by virtue of this legislation.

It is a clear breach of the Australian Consumer Law for a company ever to make a false or misleading statement about a product or service. If this legislation intends to override that then it should make that explicit. However I **recommend** that (2) should apply to all aspects of (1), so that a company is not put in the position of being forced to make a false or misleading statement.

This however raises an additional question. Can clause (1) include acts or things that are either illegal or in breach of other Australian laws? I **recommend** that a clause (3) be added, to indicate that (1) does not apply to breaching any Australian law.

This raises a further question. Can clause (1) include acts or things that, while not illegal in Australia, are illegal in the country relevant to the company? It is assumed that in most cases this legislation will be being used on foreign companies.

There are three reasons why such a situation may come up.

1. It would be entirely reasonable for country X to pass legislation making it a criminal offence for a company registered in that country to accept direction from a foreign government. This would under some circumstances make the company guilty of treason, in spirit if not in law. Country X would be looking after its own interests to pass such legislation. (If it's good enough for our MPs not to be beholden to a foreign government, why would we want our corporations to be? If we don't then we can hardly expect other countries to come to a different answer.)

2. There are countries in the world that are more respectful of human rights than the Australian government (some of which are forced to be by their constitution).

3. This legislation, if matched by other countries, is already self-conflicting. On the one hand, it demands secrecy but on the other hand it demands information.

I **recommend** that a clause (4) be added to indicate that (1) does not apply to breaching applicable foreign law.

Secrecy

The government would say that in the “good old days” every phone service was capable of being tapped, and the possibility of legally doing this, in secret, was legislated – and all was right with the world. The government would say that all that this legislation is doing is restoring the “good old days”.

However there is an important difference. Even the existence of a capability created under this legislation is secret. In fact the capability is not even specifically defined in law (hence no MP can really know what he or she is voting for).

So this is in fact a massive expansion in intrusive power for the relevant government agencies, with no judicial oversight, no parliamentary oversight, no public oversight.

I **recommend** that technical capability notices be public and that any provisions related to keeping them secret be removed. This will provide a measure of transparency about what is being done with this legislation and will allow debate about the appropriateness of the capabilities that are being created. This will also allow external expert review of the security Frankenstein that you are creating.

It is definitely worth considering this since if you get pushback from foreign corporations about carrying out your demands, you might expect even more pushback about keeping those demands secret, and find it harder to enforce the secrecy on foreign people. For example, a complex backdoor could require dozens of staff or contractors to be involved and expecting that every one of them doesn't blab might be optimistic, never mind about those staff or contractors who become aware of the backdoor some time after it is baked in.

I am specifically not suggesting that any *use of* capabilities be made public.

The transparency measure in 317ZS is laughably weak.

Likely to be used

317C Designated communications provider etc. contains several occurrences of the phrase “likely to be used”. This is unsatisfactorily vague. Assuming that it is not actually used in Australia, how is anyone to prove that it is likely to be used in Australia? Or not likely to be used in Australia?

I **recommend** that all such hypotheticals be removed. The onus should be on the government to prove that it actually is used in Australia. This is hardly an impost on the government since it can trivially make it true by itself becoming the user of the product or service. Indeed if the government is to inform itself adequately before making demands on a company, it ought to do that.

Ancillary

317C, particularly item 5, refers to an ancillary service. Apart from the obvious unsatisfactoriness of a broad term such as that, specific concerns have been raised that the government could use this to attack the integrity of the infrastructure that is used to provide secure web sites and the like.

As an example, when I connect to a bank's website e.g. https://mybank.com, there is infrastructure behind that that allows my web browser to be assured that it really is communicating with my bank, and not some imposter. That is, it assures the identity of the website. The infrastructure is not used during the communication itself in any way but is ancillary to that communication.

Breaking the fundamental trust model on which most secure communication depends would be a disproportionate response. This would be a kind of systemic weakness that the government says it wishes to avoid. I am not satisfied however that 317ZG explicitly avoids an attack on such infrastructure as the language there is somewhat general.

Along similar lines, but not quite as severe in impact, and not quite as removed from the actual communication, a DNS service could be considered ancillary to most actual network communication. The DNS service is a “naming service”.

Again, it is unclear whether an attack on the integrity of the DNS service would be considered "systemic".

For either type of service, a direct attack against the integrity of the service would have the effect of impacting a large number of users – users who are unrelated to any agency investigation – rather than impacting one or a few devices used by a person of interest.

While the Attorney General gets to decide whether something is "reasonable and proportionate", there is no real guidance as to what that means, how a future AG would decide and whether it would ever be tested in court.

I **recommend** that all items addressing ancillary services be dropped.

Failing that, I **recommend** that this section explicitly exclude "identity services" and "naming services" from ancillary services.

Really 317C and 317E together is a very bad fragment of legislation. It could be summarised as saying that the Australian parliament authorises in advance, with negligible restriction, the Australian government to require any company to do anything.

Judicial review

I understand that government is desperate to avoid independent judicial oversight of its activities. In the case, for example, of access to metadata the government might argue that they intend to use metadata hundreds of thousands of times per year and that it is not practical to have to justify the use in a court of law each time. However that must surely not apply to Technical Capability Notices.

Notwithstanding 317U it would be my expectation that adding a capability could in some cases take months (or even years if hardware changes are mandated or required), so it is unlikely that the government will be issuing hundreds of thousands of such Notices each year.

In addition, while the Explanatory Document implies that global tech companies can look after their own interests in court and contest any dodgy notices, there is nothing in the legislation that restricts the use of such notices to global behemoths. The legislation could equally be used against a single individual, where the individual may not have the resources to contest a dodgy notice. (Even where a global behemoth does contest a notice in court, it should be recognised that it is defending its own interests, not necessarily those of its customers.)

As such, I **recommend** that all Technical Capability Notices be issued by a court. That is, the government would be obliged to make the case in court, at its own expense, and satisfy the court as to the appropriateness of the notice, where the target company can choose to present its own arguments and advocates for the public could do likewise.

Along those lines, 317ZA(2) looks offensive. It should be open to anyone, including, for example, legal counsel, to suggest that a notice may not be validly issued and should not be complied with. The Explanatory Document provides no justification for this provision, no examples of when it has been required in the past or how it might be required in the future.

Costs

Since when is it reasonable that the government can decide that it is not in the public interest that 317ZK applies? I could find no other part of the legislation that would instead apply. The Explanatory Document suggests that in that case costs are not recoverable. It provides only the flimsiest example of when that might apply and the legislation certainly does not incorporate that example as a consideration in (2).

I **recommend** that the option of not allowing cost recovery be removed.

Failing that, I **recommend** that 317ZK be amended to make it explicit that costs are not recoverable in that scenario, other than as still subject to clause (15), and that (2) be amended to include the only flimsy consideration presented as an example.

I **recommend** that in 317T(12) 'applicable costs negotiator' be clarified to indicate that this is the negotiator who will negotiate on behalf of *the government* – although this is a minor point and one might reasonably infer this as the intent on the basis of other parts of the legislation. (In other words, the government can't nominate in the notice who will negotiate on behalf of the target company.)

The legislation appears to be silent on what costs are 'reasonable' or allowable. Evidently a company that must create or change software incurs a direct cost to do so. What about indirect costs such as reputational damage and loss of business?

As an example, if a Certificate Authority were forced to divulge its private key (for signing certificates) then the direct cost of doing so is relatively small but the indirect cost is massive (essentially it should close its doors). Similarly, if a website were forced to divulge its private key (for authenticating itself) then the direct cost of doing so is relatively small but the indirect cost is large (essentially noone will trust it for online access any more). Nothing in the legislation prohibits such large indirect costs.

I **recommend** that (3) be amended to clarify whether indirect costs may be claimed and, if so, to elaborate.

Maintained

317T(9) uses the word “maintained”. This word has an established meaning in software development but it is not clear to me that the legislation intends that meaning.

I **recommend** that this clause by clarified.

Systemic weakness

317ZG is not completely solid. What it says is that the government's Notice can't have the “effect of requiring” a systemic weakness. That does not mean that the government's Notice can't have the “effect of” a systemic weakness.

Stronger protection would specify that no systemic weakness may be created or worsened in complying with a Notice.

The distinction being made here could be important because putting in a systemic weakness could be the most cost-effective way for a provider to comply with a Notice.

While it may be open to the government of the day to include a specific restriction in any given Notice, there is no obligation on all future governments issuing all future Notices to do so.

I **recommend** an appropriate strengthening of the language here.

Who opens the backdoor?

The Explanatory Document (page 47) attempts to explain why a backdoor for agency access is not necessarily a systemic weakness.

One of the problems with such wide-ranging legislation is that noone can really be assured of what is being created. No MP could really know what he or she is authorising. Likewise no member of the public can really agree with the legislation. As such, the following scenario may be off the mark.

I imagine that device manufacturers will be compelled to put in some kind of backdoor that would allow agency access. The document is completely vague though on who opens the backdoor.

Does the agency have the keys to the backdoor and can open it at will, without having a technical need to involve any other party?

Does the agency identify the target device to the manufacturer and the manufacturer opens the backdoor?

From an accountability perspective, and from other perspectives, the latter would clearly be preferable.

In either case, the backdoor would be latent within the device until opened. In either case, the assumption is made that the backdoor is not opened unless doing so is legally authorised.

A problem with this legislation is that it doesn't appear to require the higher level of accountability. The legislation probably allows both possibilities so I think we all know which possibility the agencies will choose.

For the avoidance of doubt, this *is* a backdoor, regardless of who opens it. It is a clear bypass of the normal access that the owner and operator of the device would expect.

Immunity

317ZJ provides for immunity to civil liability but is silent on the question of criminal liability.

As already touched upon (in the section entitled 'Dishonest' above), I **recommend** that the legislation be amended to rule out being required to perform any act that would give rise to criminal liability, thereby not requiring any mention of immunity from such acts.

The immunity to civil liability is of course a fudge. It is not as if the government is indemnifying the provider. So effectively the other party just wears the loss.

Voluntary

I **recommend** that all parts of the legislation relating to voluntary assistance (technical assistance request and the like) be removed. A company should never put in a backdoor or otherwise act against the interests of its customers *voluntarily*. The government should not be encouraging a company to do so.

Requiring the government to compel the provider puts the interaction in an appropriate framework and makes it more likely that the law is followed, and corners not cut.

The government should not start to believe that there is any such thing as “Team Australia” and that a company is a traitor unless it voluntarily does the government's bidding.

Blackbox

317E(1)(c) appears to allow the possibility that the government could insert its own equipment or software directly into a provider's network or system, and that the provider would have to go along with that.

That sounds more like the sort of thing that a totalitarian regime would do!

(Laughably, the Explanatory Document frames this as saving the provider the cost and bother of developing the functionality.)

This raises a number of concerns.

- The effect of simply inserting a blackbox into a provider's network means that absolutely noone outside of the government can exercise any scrutiny over what the box is doing, or whether it is compliant with what limited restrictions might exist in law or not.
- This would of course once and for all give the government unlimited power to block access to whatever content it likes.
- What happens if the blackbox stuffs up and brings down the provider's network or service? Who is liable?

I **recommend** that this provision be deleted.

Future expansion

As if this legislation wasn't bad enough, 317T(5) provides for expansion by the Minister (which Minister?). This is a clear attempt to expand the legislation while avoiding public debate and scrutiny and minimising parliamentary debate and scrutiny.

I **recommend** that this provision be deleted.

If the government needs yet more power to intrude into people's lives then go back through the process of consultation and debate.

Unconstitutional?

317ZT suggests that there is some concern that some parts of 317C may be unconstitutional.

Have you taken advice over whether there is an issue? If so, please release that advice. If not, why not?

Human rights impacts

I was expecting to find in the Explanatory Document at least a token discussion of the human rights impacts of this legislation, since those impacts obviously have the potential to be very high.

Cost impacts

Likewise, I was expecting to find an assessment of the cost impacts, both on the taxpayer through recovered costs and on the consumer or shareholder through unrecovered costs.

Coughing your password

The proposed changes to Section 3LA of the Crimes Act should at least give legislators pause for thought about where we are going as a country.

- No actual justification is given e.g. examples of where people are in jail for 2 years rather than cough up a password? How many each year?
- This general provision violates the right to silence. As Australia doesn't have a Bill of Rights, that isn't a legal problem but it should be a moral problem.

- Along similar lines, this general provision violates the right not to self-incriminate.
- This provision involves a presumption of guilt, since it involves forming the view that a person is reasonably suspected of a crime, and jailing based on that suspicion, but doesn't require that suspicion to be proven in a court of law (never mind about proving beyond reasonable doubt).
- This provision will probably only ever be used when the evidence that the authorities actually have is weak. If the evidence that the authorities actually have were strong, then a prosecution could (and should!) go ahead anyway.
- A conviction can only occur on the basis that a court makes a finding about what is, or is not, in someone's head.

The potential for a miscarriage of justice should be obvious!

You would wonder whether this provision could give rise to a new form of malware, which scatters files with genuinely random content around the place.

It is laughable that a person could go to jail for more years for forgetting a password than for the underlying (alleged) crime. At the very least, I **recommend** that the maximum jail sentences given in the amended 3LA(5) and introduced 3LA(6) should be limited to the maximum that applies to the alleged crime.

Even so, it's a bad look. “We have a weak case. You could go to jail for 3 years if we get a conviction but we can't because our case is too weak. So we'll jail you for 3 years (or 10 years, per the actual proposed legislation) anyway, even though we can literally never prove that you know the password.”

In considering this amendment, it is helpful to look at the Rawls case, notwithstanding that that is a US case.

Rawls has been held in custody for almost 3 years to the day. He has not been tried. He has not been convicted. The authorities claim that he knows the password. He claims he doesn't.

There are some differences between the US and the proposed or existing Section 3LA.

- In the US, a suspect can be held indefinitely without trial. Life imprisonment without trial! So the Australian legislation is not quite as bad as that.
- In the US, because they actually have a Bill of Rights, this provision can only be used when it is a “foregone conclusion” that the password will yield incriminating evidence. That is a substantially stronger threshold than the threshold that applies in Australia (reasonably suspect etc.) So that's a strike against Australia.

One aspect that is not clear to me is whether the government could apply 3LA repeatedly i.e. jail someone for up to the maximum permitted number of years, let them out, and then apply again to a court over the same piece of potential evidence. On the one hand that probably subverts the intent of the law but on the other hand I didn't see anything explicitly ruling it out.

If this is currently possible, I **recommend** that the section be amended to rule it out. For any given crime and suspect, 3LA should only be able to be used once.

Whether the government could use 3LA to jail someone for life could depend on satisfying a court that the person *still* knows the password after each jail sentence. In fact this is a general problem with this law and with the Rawls case. A person may have known a password at some time in the past. Even if so, that provides no guarantee that a person knows a password at the current time.