1300 848 333

28 October 2019

For the attention of the Independent National Security Legislation Monitor (INSLM)
Dr James Renwick CSC, SC

Submission to the INSLM review of the Telecommunications and other Legislation Amendments (Assistance and Access) Act 2018

Dear Dr Renwick,

I am an independent cybersecurity consultant of some 18 years' experience. I started my career in IT Canberra almost 20 years ago, where my first job was working in a classified government environment as a firewall administrator. I moved on to DSD certified Internet gateways, and eventually away from Canberra and into the corporate world where I was exposed to a wide array of industries including top tier hardware vendors, VOIP, banking and financial services, and even online wagering. More recently I have focused my efforts on helping small business to start taking cybersecurity more seriously.

The trajectory of my career has given me a uniquely broad understanding of cybersecurity as it applies in almost any context. Ever since IT security first emerged as a distinct discipline, I have watched successive governments from both major parties make ill-conceived attempts to try regulate the Internet and associated technologies when they clearly did not understand them, and had not even bothered trying to educate themselves about them. Invariably these efforts are at the behest of un-elected, self-serving bureaucrats pushing their own narrowly focused departmental agendas. The result is always bad policy which does nothing to achieve its publicly stated aims, but does further tighten the grip of these would-be despots on the levers of power at the expense of the rest of the Australian population. TOLA is only the latest example of this.

I make this submission in response to your October 21 article in the Australian Financial Review "Time for industry to speak up on Australia's encryption legislation", and will specifically aim to address the four important questions you ask in the article. I had not planned to make a submission to your inquiry, but with so few people speaking up, and members of parliament debasing themselves by stooping to rabid hyperbole such as loudly proclaiming under parliamentary privilege that anyone opposed to the laws is on the side of terrorists and child abusers, I believe it is important to correct some of the misinformation propagated by the government which has framed the debate so far.

As to the questions raised in your article, I provide the following answers:

**Is the law in any respect too wide, too intrusive, or lacking in sufficient safeguards?**

TOLA is unquestionably too wide and too intrusive. The need for this legislation has consistently been justified by the government as a means to fight terrorism and child abuse. In reality, the letter of the law has made it applicable to any "serious crimes", defined as any offence with a maximum prison sentence of 3 years or more. This obviously encompasses a much broader range of offences than terrorism or child abuse, and includes offences which are clearly not a threat to anyone's personal safety such as copyright infringement and fraud. If the government had been serious about their intentions for the applications of TOLA, they would have created a very specific list of offences related to terrorism and child abuse to which the powers the act grants can be applied. Instead

they have intentionally broadened the scope so they can be applied to almost any criminal investigation.

The wording in the act also effectively allows the government to serve orders on almost any person or organisation by using an intentionally vague definition of "designated communications provider" as any party that "provides an electronic service that has one or more end-users in Australia." By this definition, anyone with a WiFi hot spot or a website is a designated communications service provider.

Aside from this kind of scope creep, TOLA states that orders can be made under the act for "assisting the enforcement of the criminal laws in force in a foreign country". This effectively allows an Australian citizen who has broken no laws in Australia to be targeted by a foreign government using our domestic legal system. This is an affront to our national sovereignty, but more embarrassingly it betrays one of the true motivations behind TOLA – to appease the American intelligence agencies. It is a poorly kept secret in the information security community that the history of TOLA begins with the Americans trying to convince New Zealand to implement similar laws, and only when they refused did they turn to their friends in our own security agencies, who were sadly only too eager to help out.

As to whether TOLA has sufficient safe guards, considering there are none, the answer is clearly no. Orders made under the act are authorised by the same agencies which issue them – that is not a safe guard, that is a clear conflict of interest. In fact, everything in the act which might constitute a check on this power boils down to the subjective assessment of the head of the agency that issued the order in the first place. There is no independent or judicial oversight, and the avenues for dispute or appeal are heavily constrained by the inability to get external legal or technical advice due to the excessive confidentiality requirements of the orders, and the fact that the government can simply say the matter is urgent to force immediate compliance. In any other context this kind of self-serving behaviour would be considered blatant corruption and abuse of power.

The idea that requiring the Attorney General and/or the Communications Minister to approve a TCN somehow counts as proper oversight is a bad joke – they are both political operatives of the same governing party, unlikely to disagree with each other in any event, and by no means independent. They will be completely within the law to use the power granted under the act for their own political benefit, and no one would be able to stop them. The final irony of this is that the one class of people the politicians saw fit to exempt from the intrusions of TOLA is politicians, ensuring they will never be subject to the kind of scrutiny that the rest of us are. This exemption is a clear example of a corrupt government seeking to avoid scrutiny.

One of the biggest dangers of TOLA that has been overlooked in much of the debate so far is that it empowers the government to co-opt the domestic private sector into creating a mechanism for total surveillance that once in place will be almost impossible to remove, but very easy for future governments to abuse or expand. This was the driving reason behind public opposition to Labor's Internet filter, and the same reasoning applies here. With TOLA already passed, we face an uphill battle to wind back this governmental over reach before it becomes so entrenched that the agencies responsible simply claim that it cannot be done.

The risk to our democracy by powers like those granted TOLA cannot be over stated. The only thing that stops them from being used as tools for oppression and political manipulation or suppression is the good will of the people in charge of them, but the government and its agencies have demonstrated time and time again that they cannot be trusted to do the right thing, whether it is raiding journalists for reporting on government corruption, using the metadata retention system to stalk ex-lovers – we know this sort of thing goes on, the government would like us to accept that this is a reasonable price to pay for the "safety" they afford us by violating our human rights every day.

**Does the law have disproportionate or unintended adverse effects on Australian industry?**

The passage of TOLA had an immediate effect on the reputation of Australian tech businesses internationally, and negatively impacted on our ability to compete on the global market. As someone who is engaged with the Australian start-up community, and is highly active in the local cybersecurity community, I can say that I have heard first hand from multiple business owners who have tried to take their products overseas, or seek international investment, only to be told up front that their products were no longer marketable due to TOLA passing, or that they would have to move their operation off shore to secure investment.

In short, TOLA makes it unviable to run a technology business in Australia. Given the current challenges of the Australian economy and its reliance on primary industries which are in decline, it is incredibly destructive to Australia's economic security to implement laws which effectively kill off any prospect that we can transition to a more modern knowledge-based economy.

There is also the question of cost for compliance with orders made under TOLA – both monetarily, and in opportunity. The act has some provisions for a recipient of an order to recover costs from the government, but the act has completely failed to consider whether the financial burden of redirecting resources to fulfil the request could be sustained by the business. The reality is that the effort required to implement the kinds of significant changes which can be ordered under TOLA would likely send most Australian businesses bankrupt long before they were able to recover any costs from the government, not to mention any legal fees they might incur in the process of disputing an order.

Aside from the financial cost of implementation, there are no provisions in the act for a business to receive compensation for missed business opportunities that result from having to divert resources to complying with a TOLA order. What happens to a business that misses out on a $50000000 deal because they are preoccupied with a TOLA notice? What happens to their reputation and future opportunities when the word gets out that they walked away from such a big deal for no apparent reason? What happens when the news leaks, as it inevitably will, that the company was actually subject to a TOLA notice, and everyone single one of their existing customers dumps them over night? The cost implications are far wider and longer ranging than the simple cost of technical implementation.

It is imperative for our national economic security that TOLA be repealed. While there is no arguing that law enforcement needs modern tools, capabilities, and perhaps even new powers, to deal with modern criminals and threats, they cannot come at the expense of our long-term economic stability. The government and law enforcement agencies are simply seeking the solution which is the least amount of work for them by pushing the responsibility and the burden for implementation onto the private sector.

**Does the law in fact undermine lawful encryption, say in banking?**

Given that the scope of what can be compelled under the act is effectively only limited by what is technically feasible to implement, the answer is certainly yes. The quaint fiction promoted by law enforcement agencies that it is somehow possible to have strong protections for our own technology while weakening the protections of those who seek to do us harm ignores the fact that we are all protected by the same technology these days, all based on the same fundamental principles and technological building blocks. The luxury of facing adversaries with fundamentally different encryption is a relic of the Cold War that no longer applies. The world has gotten smaller and the Internet has normalised the spread of technological advancement.

The government and its various agencies have consistently sought to deliberately mislead the public about the nature of TOLA – for their purposes it is important that the fundamental issue at stake be seen as one of national security vs personal privacy, as they can then strongly argue that national security – safety for all – must trump the right to personal privacy. It also provides a more palatable justification for the public to introduce these measures, which under other circumstances would be considered draconian tools for totalitarian regimes.

The true nature of TOLA however, is that it is not a matter of national security vs personal privacy – it is one of national security vs a different kind of national security. Given that the cybersecurity technologies which protect our banking, our hospitals, our elections, and our critical infrastructure are exactly the same as the ones used by terrorists and child abusers to stay hidden from law enforcement, the powers granted under TOLA to compel the creation of weaknesses or removal of protection in cybersecurity technologies are therefore a trade-off between the kind of security that comes from everyone being able to communicate securely, or no one being able to. The former protects our economy, our personal information, and critical infrastructure from cyber-criminals and state sponsored cyber-attacks, the latter may protect us from terrorists, child abusers, and other people who seek to do us harm by enabling the government to spy on them – and everyone else at the same time.

The government are desperate to avoid public discourse of TOLA as a choice between different aspects of public safety, not only because it neutralises their argument for the necessity of TOLA in the first place, but because it changes the point of contention from one that is easily portrayed as good vs evil to one which is morally ambiguous, and consequently undermines their ability to claim their ideology and motivation is righteous. They know that without this advantage they will struggle to find supporters for legislation that fundamentally infringes on the human rights of every Australian, and permanently shifts the balance of our "democracy" to further entrench the power of politicians and bureaucrats who already act as though they are accountable to no one.

The inconvenient truth of TOLA is that there is no middle ground, the alternatives are mutually exclusive. We all are riding in the same boat now, knocking holes in the hull to sink the pirates will only see us drown ourselves as well.

It also cannot be ignored that the government has flat out lied about its ability to keep the kinds of vulnerabilities it wants to introduce out of the hands of cyber criminals and state sponsored hackers. The NSA could not stop its exploits and tools getting stolen and used by botnets to infect millions of computers around the world (e.g. Eternal Blue), our government will be no different.

**Is the law expressed in terms likely to remain relevant as technology changes?**

Strictly speaking this is impossible to quantify because we cannot know how technology will change, but again, if history is anything to go by the answer will likely be no. However, I do not believe this is the right question to ask. There is a danger in trying to write laws to account for things we cannot anticipate, in that the more generalised they become in seeking to account for such eventualities, the more likely it is that there will be unintended consequences, that they will be abused or applied in ways never intended by future governments, or even the private sector.

For this reason, I would actually suggest that seeking to make laws which remain relevant over time is actually counterproductive and harmful to society. Laws must evolve with the rest of society, or they simply stifle our ability to grow, change, and innovate. Worse, they become tools for depriving people of their rights and controlling the progress of society to suit the whims of the privileged – just look at what we had to go through to get marriage equality. It is therefore imperative that any technology based legislation have expiry dates for the applicability written into them, so that parliament is forced to be proactive in keeping such laws up to date with modern technology, and modern threats.

Finally, I would like to suggest that perhaps the most important question, is one you didn't ask:
**Will the laws achieve the outcomes the Government claims?**

Throughout the whole debate on the AA Bill and now TOLA, the government has failed to adequately answer one simple question – how will these laws actually be effective against terrorists and child abusers? The reason for this failure is simple – they will not be, and the government knows it. Regardless of what Australian law says, the Australian government cannot compel American Internet giants, or Chinese ones for that matter, to do anything. They cannot compel open source projects to do anything. They certainly cannot compel terrorists and child abusers to use Australian

products now that it's public knowledge that they aren't trustworthy. Even assuming the government was able to convince the likes of Facebook to cooperate, the people TOLA seeks to capture have plenty of other options at their disposal, including creating their own tools which the government has no visibility and no understanding of. All TOLA will do in the long run is make those people harder to catch by driving them away from commodity products, while making the rest of us more vulnerable.

In closing, I will ask that you consider the whether the vaguely defined benefits of TOLA are really worth the costs to our society that come with it. I believe that the inescapable conclusion is that economically, technologically, democratically, and defensively – we can't afford it.

Regards,

Corch

Managing Director

Shogun Cybersecurity