Submission to the INSLM Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 (TOLA Act)

Dr Chris Culnane and A/Prof Vanessa Teague
School of Computing and Information Systems
The University of Melbourne

September 2019

The opinions expressed in this submission are the authors' own and do not reflect the views of The University of Melbourne. We concentrate on the somewhat-technical aspects of Schedule 1, though we agree with many of the concerns expressed about the other schedules also.

1 Introduction

In this submission we will reiterate a number of concerns raised previously to PJCIS inquiry and publicly with regards to the contents of the TOLA Act.

Whilst there is a clear need for the protection of society from those who seek to harm it, such protections must not result in the erosion of the very values that are supposed to be being protected. Australia prides itself on being a free society that values dignity of the individual, so much so that it is in the values statement published by the Department of Home Affairs: "Australian society values respect for the freedom and dignity of the individual,..."[1] As such, one is forced to ask whether the TOLA Act is consistent with protecting those freedoms or acts to undermine them. There is no victory in eroding those core values for only incremental improvements in security and protection.

We will lay out in this submission reasons why we believe that the current balance is incorrect, and that the TOLA Act not only erodes those freedoms, but fails to provide even an incremental improvement in security when faced with a moderately capable adversary.

2 The risk of undermining cybersecurity

A well-intentioned police or intelligence operation designed to expose the data of just one individual might accidentally introduce a security problem that exposes other users' data to attack. The TOLA Act contains some efforts to mitigate this risk, but they do not adequately protect the security of innocent users. We give two specific examples below.

[1] https://immi.homeaffairs.gov.au/help-support/meeting-our-requirements/australian-values#content-index-2

2.1 Technical Assistance Request Limitations

One of the few amendments that was made to the Assistance and Access bill prior to its enactment was to include Technical Assistance Requests in Division 7 - the part of the legislation that acts to limit what actions can be asked for under the legislation. Prior to the amendment being included the TARs were excluded entirely from Division 7, as such, their inclusion in at least some form is a step forward, however, the amendment fails to appropriately or consistently limit TARs. The primary issue is that TARs have been bundled with the limitations applied to TANs - the Technical Assistance Notices. Such notices, as a result 317L(2A), are limited to not requiring the development of new capabilities "The specified acts or things must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency". However, no such restrictions applies to TARs, which can request the development of new capabilities. As such, TARs are more closely aligned with Technical Capability Notices (TCNs), albeit that they are voluntary. The distinction is important, because TCNs are not permitted to request the development of a new capability to remove electronic protection, more specifically, they cannot request an act or thing as described in 317E(1)(a).

The end result is that TARs remain the broadest form of notice or request, with the possibility of requesting the development of new capabilities to remove electronic protection. This is particularly risky because those electronic protections might also be relied upon by other users. The counter point that TARs are voluntary holds little sway: if something is not acceptable to require, it should not be considered acceptable to request either, particularly given the request process is shrouded in secrecy, removing any notion of public scrutiny.

2.2 The definition of systemic weakness

Damage to the cybersecurity of ordinary users was meant to be prevented by prohibiting the introduction of a *systemic weakness*. However, discussion around the legislation has been consistently dogged by the ambiguity around the definition of *systemic weakness*. This is not a term that has a history of wider use, and the definition within the legislation is ambiguous. This too was an area that received an amendment prior to the bill passing, but the amendment does nothing to address the ambiguity and in fact makes very little sense. The amendment introduced two definitions, one for systemic weakness, and one for systemic vulnerability:

> "*systemic vulnerability* means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified."

> "*systemic weakness* means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified."

The first point of note is that the definitions are identical, except for the word vulnerability in the first definition having been replaced with the word weakness in the second. It should not come as a surprise that the definitions are identical—vulnerability and weakness are synonyms in ordinary English. More importantly, neither definition actually defines its key term. What is a vulnerability or weakness exactly? What one person regards as a weakness might be described by another as a helpful information-sharing feature.

2.2.1 Class of Technology

The second issue is in regards to the definition what a *class of technology* is. The definition blocks a vulnerability that affects a whole class of technology, but immediately excludes target technologies that are connected with a particular person. The first problem with that is there is no definition of what a *class of technology* even is. It is not a term that exists in technology literature. A reasonable reading would be to assume that *class of technology* would be so broad as to be all mobile phones, or all ADSL connections, or all social media. The problem with such a definition is that no TAR/TAN/TCN could ever be issued to a single organisation that controlled an entire class of technology, since no such organisations exist. Therefore a TAR/TAN/TCN will never cover an entire class of technology. Crucially it does not state a class of technology offered by a specific provider. If it did, it would prevent a single provider having to weaken its entire service or network. Without such a clause it would appear that it will be perfectly legitimate to ask a telecommunication provider to introduce a vulnerability to the whole of its network, since that will not cover an entire class due to other telecommunication providers not being included in the same TAR/TAN/TCN.

2.2.2 Target Technology

A further problem occurs when looking at the longer definition of target technologies. It appears to cover almost anything, provided it is being targeted at a particular person. For example, part of the definition states:

> "for the purposes of this Part, a particular carriage service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a target technology that is connected with that person;"

If a carriage service can be a target technology that would indicate a very broad view of *class of technology*. A carriage service would encompass all traffic going through a service provider's network. As such, it would appear that the definition of *systemic weakness* and *systemic vulnerability* do not even preclude the building of bulk interception capabilities for a carriage service provider, providing at least one person of interest is using that service provider. Furthermore, the latter part of the definition of *target technologies* states:

> "For the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is immaterial whether the person can be identified."

If it is immaterial whether the target person can be identified, that implies that the legislation would permit bulk interception. Furthermore, it would seem to call into question whether the notice or request is about a particular person, if that person cannot be identified. Additionally, since the definition of *target technology* only requires that it is *likely* to be used by a particular person it could be entirely speculative.

2.2.3 Other definitions within the same Act

The limitations in Section 317ZG do include a reference to actions that "jeopardise the security of any information held by any other person." This sort of phrasing might have formed part of a good definition of prohibited actions if it had been the main definition. As it is, it is very difficult to understand how it relates to the other definitions discussed already. It might set a more protective boundary around innocent people's data, or it might merely add to the confusion.

2.3 Summary

The amendments made to the bill before it was enacted have done little to address security concerns or eliminate ambiguity. If anything, they have made a number of matters worse. The risk that the legislation could be used to perform bulk interception is of particular concern. If we look at examples from the US[2] and the UK[3], both have struggled with legislation that was supposed to be targeted but has resulted in bulk interception.

The combination of terms that are not in common usage with no or ambiguous definitions would be a concern in any legislation. In a piece of legislation that will be utilised largely in secret it raises particular concern. The usual public scrutiny of its application will not take place, and as such, if ever there was a piece of legalisation that should have tightly written definitions and unequivocal limitations it is the TOLA Act.

3 Is it proportionate?

The question, "Is the TOLA Act proportionate?" isn't well defined either. We assume it means whether the problems it introduces are (at most) proportionate to the likely benefit it gives. We have argued above (like many others) that the problems are serious. We now examine the likely gains.

We do *not* believe the possible harms of the TOLA Act should be judged against the fear of terrorism, or the harm done by paedophiles and organised crime. Clearly these are enormous, but the TOLA Act will not make them disappear. When we consider whether it is proportionate, we should ask whether the harm it does to security, privacy and freedom is proportionate to its *likely effectiveness* in fighting serious crime.

3.1 How effective will it be?

We can only speculate as to what its success in detecting and preventing serious crimes will be. However, we can apply the same security analysis techniques that we would apply to proposed security protocols to form an informed judgement. In particular, we can take an adversarial view and speculate as to how an adversary could circumvent or avoid the powers created in the legislation. If it is possible to construct a plausible strategy that the adversary could use, we should assume that such a strategy will at some point be adopted, and as such, any gains claimed by the legislation will be lost. This is particularly important with regards to determining whether the legalisation is balanced. There should be an implicit benefit today, since the adversary has yet to adapt to it, however, for the legalisation to have net gain, any benefit must continue to exist even after the adversary has had a chance to adapt. It is our opinion that a reasonably competent adversary could avoid the risk of interception with minimal technical knowledge, and the use of commodity off-the-shelf components. If that is the case, any benefit would be greatly reduced, nearing zero, with a high price paid in terms of privacy, freedom and cybersecurity. Such a trade-off should be considered to be unacceptable in a modern functioning democracy.

The details of our analysis are provided in Appendix A. They are separated from the main body of this submission under the expectation that they will not be made public, as whilst we consider a similar approach could be taken by any competent adversary, there is no desire to assist them in that regard.

[2] https://www.theregister.co.uk/2018/08/06/us_spying_programs/

[3] https://www.computerworld.com/article/3427019/the-snoopers-charter-everything-you-need-to-know-about-the-investigatory-powers-act.html