Science Party
PO Box 20409
secretary@scienceparty.org.au

Office of the Independent National Security Legislation Monitor
INSLM@inslm.gov.au

1st November 2019

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

Thank you for the opportunity to comment on the *Assistance & Access Act 2018*. This submission was prepared by Dr Andrea Leong and Dr James Jansson on behalf of the Science Party. This submission does not need to be kept confidential and may be made public.

Dr James Jansson is a full-stack developer, founder of startup *Tapview* and currently a senior developer at an Australian software-as-a-service provider for the medical industry. He is also the Deputy Leader of the Science Party.

Dr Andrea Leong is a privacy advocate and the Leader of the Science Party.

1. Summary

The Science Party recommends that the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 be repealed entirely.

Some arguments that follow were presented in the Science Party's comments[1] on the Assistance & Access Bill, submitted to the Department of Home Affairs on 10th September 2018.

2. Security concerns and international obligations

Privacy is security

The dichotomy between privacy and security is a false one: threatening the integrity of encrypted communication puts all Australians at risk. Specific concerns include creating a large single repository of Australian citizens' personal data, regardless of whether they are suspected to be involved in illegal activity. This represents a uniquely attractive target for bad actors. Citizens' telecommunication data should be subject to surveillance only on the basis of a warrant to do so.

[1] 'Comments on the Assistance and Access Bill'. Science Party. https://www.scienceparty.org.au/comments_on_assistance_access_bill

The compromising of security systems could lead to the publication of highly sensitive personal information, including:

- Medical information that could reveal, for example, a person's sexual activities
- Financial information that could lead attempted identity theft to steal from a person, or could lead to kidnapping, hostage situations and murder
- Geolocation information, which could allow criminals to establish a live location for a person, or allow them to determine a pattern of habits for an individual

These are just a few examples of how weakened security and the unnecessary storage of personal information on government computers could lead to serious threats to the physical safety of Australians.

Private communication promotes open democracy

Knowing that the content of our encrypted communications might be intercepted can be expected to have a chilling effect on whistleblowing and investigative journalism into subjects that are embarrassing for the government. This is especially true in a culture that has shown itself to be hostile to whistleblowers and quick to raid journalists' homes and offices.

Protections against warrantless spying should not take the form of exemptions for journalists and their sources, but extend to all citizens.

Surveillance laws could be counter-productive to their aim

The stated aim of many national security laws is gathering of intelligence, but laws that threaten encryption could prejudice Australia's agreements with other countries' intelligence-gathering programs. For example, concerns have been raised about potential incompatibility between the Assistance and Access Act and the USA's CLOUD Act.

Lack of strong evidence of failure to comply with voluntary requests

Australia's security agencies have failed to report cases where a company or individual has refused to comply with a request to assist them with preventing or prosecuting a serious crime. Although we accept it would likely harm investigations and national security to reveal all of those details, it would be informative to have a simple tally of all of the times that an ASIS, ASIO or ASD agent asked an Australian-operating company for information or assistance and it has refused.

3. Technical and legal issues

Open source projects

Open source projects provide a particularly tricky set of circumstances for technical assistance notices (TANs) and technical capability notices (TCNs), as the code for these projects is publicly available. It will be evident that a notice has been made and who has implemented the request. Reputational damage to both the company and the developer for being revealed as having implemented a state-demanded exploit could be substantial.

When making notices to open source projects, additional consideration should be given to the publicly-available nature of the code involved.

Source control — a permanent history of national security operations

Source control tools, such as Git hosted on GitHub, GitLabs or Bitbucket, provide a convenient method for collaborating with colleagues and keeping track of all changes in a code repository. As coder writes code, they check this code change into the repository, which may be then reviewed by a supervisor and which finally results in an automatic deployment of the code to a server.

If developers are asked to make a change to the code to comply with a notice, this change may be permanently recorded in a source control tool. When determining if a notice is onerous, attention should be paid to how much the change interferes with the industry-standard of using source control tools to manage code and preferably, solutions should be sought that are short-lived and easily reversible to avoid permanent records of the changes being hidden in the repository.

Issues around foreign national employees

If a company that employs foreign nationals is served a TAN or TCN, those foreign national employees might be removed from a project because doing so may expose them to information about the national security operations taking place in the company. Similarly, many companies outsource substantial parts of their work to off-shore developers.

Implementing a change to the code may result in that code no longer being appropriate for people who would not pass a security background check. Given that wages are a substantial cost to companies, forcing employees to be cleared for national security work could substantially increase the costs to a company.

When determining whether undue regulatory burden will be applied, particular attention should be placed on whether the notice will result in increased wage costs. Those wage costs may extend beyond the timeframe of the national security operation if records of those national security operations are retained within the company either in the code base or in administrative records.

Companies that suddenly fire all of their foreign employees may be inadvertently revealing that they have been served with a notice related to national security. This could be a security risk both for the national security operation, for the company and its employees.

Compliance issues with foreign law

Laws regarding data integrity and privacy (especially those in the European Union) could make Australian software and software-as-a-service providers ineligible for both government and private contracts for the management of health data, financial records and communication data.

There are currently no provisions that limit the issuance of notifications to only affect residents of Australia, meaning no Australian company can give meaningful assurances to foreign governments and companies that their code is free from exploits or that their data would be protected from warrantless inspection from Australian spy agencies.

Insufficient protection against lost profits

The act talks about compensation for lost productivity of individual companies due to the issuance of notices, and allows for appeals based on excessive regulatory burden. However, the act makes no mention of compensation of lost revenue due to the act itself. The act itself has created a very large regulatory burden on all Australian software and software-as-a-service companies, especially if access to foreign markets such as the European Union is impacted.

Complications around liability

The act does provide for exemptions for civil liability where the thing done by the provider was in compliance with a TAN or TCN. However, there are probable scenarios not covered by these exemptions:

1. Foreign civil liability

Most modern companies providing the kinds of services that would qualify them for being asked for assistance will be either currently in or planning to enter foreign markets. The civil liability potentially due to foreigners could dwarf the potential civil liability to Australians, as Australians make up just 0.3% of the world's population.

Given the tacit admission in the bill that there is potential for harm through the application of requests, it should be negotiated with other major trading partners to extend that protection, or for the government to provide foreign civil liability insurance up to a set amount or proportion of the amount the company may be sued for.

2. Using notices as a defence is technically difficult and could harm confidence in Australia's justice system

If a company is sued, for example, for a data breach that is ultimately caused by works undertaken as part of a TAN or TCN, the company may defend itself by relying on civil liability exemptions in the act.

A major problem with this is that having the case dismissed, especially one where many parties are involved, would result in strong suspicion that a company was the subject of a notice. This revelation may be bad for national security or for the prosecution of crimes. The alternative, to have to case rejected without revealing why, could cause the courts to fall into disrepute, which would be bad for democracy and justice in this country.

3. No protection against criminal cases

The law is unclear as to where people who comply with notices stand with regard to violations of other laws.

The holes in this legislation are manifold and irreparable, and for that reason the Science Party recommends repeal of the bill.