June 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Submission to the Parliamentary Joint Committee on Intelligence and Security review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

I note that the Committee has resolved to focus on the following aspects of the legislation (the Terms of Reference for this review):

- the threshold, scope and proportionality of powers provided for by the Act;
- authorisation processes and decision-making criteria;
- the scope of enforcement provisions and the grant of immunities;
- interaction with intelligence agencies other powers;
- interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*;
- impact on industry and competitiveness; and
- reporting obligations and oversight measures.

I will comment on each of these terms of reference in turn below. In addition, I have included as appendices to this submission, my submissions to the previous review of this act.

In summary, I maintain that the entire framework of the Technical Assistance Request, Technical Assistance Notice, and Technical Capability Notice defined in this legislation should be repealed, and that the amendments in relation to search and surveillance provisions in the act need to be significantly amended for the act under review to be considered measured and reasonable.

**Threshold, scope and proportionality of powers provided for by the Act**

1. The act declares that a person (not a member of the security forces) can be "requested" to provide information or assistance to law enforcement officials. These requests of a person are required to be kept secret under threat of (harsh) penalty, and are required to be complied with under threat of (harsh) penalty. Complying with any such request will typically violate security and access control policies of any organisation, will typically result in log and audit entries, and may trigger internal security alerts which will be investigated.

   Further, the legislation permits "unknown" changes to be implemented by law enforcement officers, which in turn potentially introduces unknown (and un-testable) vulnerabilities into an organisations infrastructure.

   Any person providing such information or assistance will then likely be subject to disciplinary proceedings within, or dismissal from an organisation. This act has put any such person in an untenable position.

   Any requests for such information or assistance need to be able to be reviewed by information technology peers and any necessary management and / or legal opinions or approvals sought. The person (or organisation) *must* be able to decline such requests without penalty.

   These provisions must completely repealed, or re-written such that they apply only and explicitly to organisations or people knowingly complicit in the offence(s) being investigated.

2. The act permits "adding, copying, deleting, or altering other data in the target" without adequately defining what limits or scope any changes must fall within.

   Adding must be restricted to the making of a copy of some data, and modifying must be limited to standard operating system changes to meta-data (eg. the timestamp of the last access of a file).

Any deletion powers under the legislation should be limited to deleting copies of data created in the process of investigations conducted within its' terms. There should be no case where the content of a file or data content is in any way altered (editing), created (adding), or deleted.

The act should not permit changes to the configuration of the computer system (for example, network routing, firewall settings, user account settings, etc.).

The current language of the legislation is far too broad, and could readily be interpreted to allow pretty much anything to be done to any data on a "target".

3. The legislation is fatally flawed in that any measure implemented can be readily bypassed by even relatively technically illiterate users. It might catch an inept actor, but any organised actors will simply switch to known (readily available) secure technologies, and leave law abiding users using compromised technology for little or no gain in the security, and probably significant cost to commercial organisations.

   For example, let's assume that Australia manages to get Facebook WhatsApp to implement measures to allow its' law enforcement agencies access to the communications of target actors. The target actors could simply switch to a more secure application (for example, Signal, which has publicly stated that it will not compromise its security to comply with foreign state actors such as Australia!), or utilise anonymous proxy servers, configure virtual private networks, etc. Alternatively, the target actors could encrypt messages off-line and then still utilise a compromised WhatsApp to securely send content, though leaving a meta-data trace, or they could simply switch to an open-source or proprietary (in-house) technology based on the available specifications for services such as WhatsApp, OpenPGP, OpenSSH, and many many more.

   The legislation will not provide Australia's' law enforcement with visibility of the communication of other than the general public and inept criminal actors. Any determined criminal actor will simply switch to alternative available technologies.

   This legislation seeks to target commercial software and applications which can be used for criminal activities by providing information or assistance to permit access to pre or post encrypted data held by or transferred between entities. Whether the legislation requires entities to decrypt communications or circumvent encryption technologies, the effect is the same: Secure communications technologies become insecure.

   The access mechanism implemented to permit "secret" access to data is called a "back door". Such back doors will most certainly be exploited by hostile actors, and will therefore do far more harm than good. The security agencies are pushing the view that these secret back doors are secure because they are secret, despite the fact that "security through obscurity" is widely accepted as "false security".

   Implementing secret access mechanisms for law enforcement in the name of "national security" weakens the security of everyone, and imposes not insignificant development and compliance costs on developers and vendors, and will do nothing to disrupt determined criminal actors.

4. Australia was assured that access to the retained metadata required to be collected under earlier legislation would be carefully controlled, and only used for investigations of serious criminal activities by a very limited number of our security agencies. This has been shown to be a promise that has been unable to be kept.

   The review needs to recommend that access to retained meta-data be the subject of a valid warrant which is granted under provisions similar to those required for search, surveillance, and seizure warrants. In particular, meta-data in whistle blower actions needs to be strongly protected, and should not be easily accessible to anyone without suitable judicial oversight.

**Authorisation processes and decision-making criteria**

1. It should never be acceptable that "wrongs" or information in the public interest can be hidden behind national, or for that matter, corporate security and secrecy provisions. The first test in any

investigation of information disclosures must be whether the disclosure satisfies the conditions of public interest. Only if the disclosure fails that test should any investigation proceed further. Public interest should include any actions which would be judged to be illegal, corrupt, biased, or likely outrage community or society (eg. abuse of power, internal reports or actions which conflict with the public perception (think Tobacco industry, gas exploration, …), communications or actions of subversive elements, ... (I'm not a lawyer, but I'm sure others could better define what would be in the public interest).

To misquote Edmund Burke (ref: https://quoteinvestigator.com/2010/12/04/good-men-do/) - "The Only Thing Necessary for the Triumph of Evil is that Good People Won't or Cannot Act", or to misquote Thomas Jefferson - "All tyranny needs to gain a foothold is for men of good conscience to be silent or silenced."

Australia (indeed, any democracy) needs strong "whistle blower" legislation so that any wrong-doing by any entity, or information in the public interest, can be brought into the light - to the attention of society and authorities. Protections should exist for those who make factual disclosures in the interest of Community, Society, Environment, or Nation. Any legislation to address this situation should not provide special case provisions (for "the media" for example) - it should apply equally to anyone who blows the whistle.

There must however be independent organisation(s) through which such information can be channelled, and which have the resources and incentives necessary to pursue and expose the issue with and on behalf of whistle-blowers. The use of such organisations should not be a prerequisite for "blowing the whistle", and whistle blowers should be able to remain anonymous (think "Crime Stoppers" where crimes can be reported anonymously). In a democratic society, the independent media organisations would be one such channel, but should not be the only channel. Other possible channels might include an ombudsman, politicians, police, labour unions, environmental groups, or any other group that has an interest in exposing information in the public interest or prosecuting wrong-doing.

A fearful and timid public is a pre-requisite for a corruption and misconduct. The current legislation has demonstrably been applied (eg. AFP raids on media organisations) to intimidate potential whistle blowers. Without strong whistle blower protections, this legislation will inevitably lead to corruption and criminal conduct because no-one will be able to safely expose such conduct. Legislation in a democracy should work towards transparency in its' intent and application. A number of commentators have commented that our current legislative path is headed in the opposite direction – marching Australia towards a Police State. One respected international commentator asked "Is Australia the world's most secretive democracy" (New York Times, 5 Jun 2019: https://www.nytimes.com/2019/06/05/world/australia/journalist-raids.html). The former human rights commissioner Gillian Triggs said, Australia is now the least observant and the most repressive of the Western democracies. (PM, ABC Radio, 5 June, 2019) This is not the direction we should accept.

2. All active actions (assistance, surveillance, seizure, detention, …) under this act (and in fact, all legislation!) must be approved by an independent (judicial) authority in the form of a warrant to perform specified actions against targeted individuals or organisations that have come to the attention of authorities because of *documented* indications (evidence) of past, on-going, or planned unlawful activity. This requirement is also needed for access to meta-data. Protections should apply to prevent a warrant being issued to investigate whistle blower actions.

   A judicial officer issuing a warrant must be familiar with the law(s) pertaining to the unlawful activity being investigated, the laws pertaining to the powers granted under the warrant, must be satisfied that the evidence supporting the request for the warrant is sufficient to support the actions authorised under the warrant, and that there is a very high likelihood that evidence acquired would contribute to a conviction and / or disrupt the unlawful activity.

All warrants must be able to be challenged (for example, on the evidence presented when a warrant is being sought), and any evidence collected under or consequentially because of an improperly issued warrant should be inadmissible. This would ensure that the authorisation of a warrant needs to pass a test based on documented evidence available that would justify the actions authorised under the warrant.

3. There should be no power to compel law abiding individuals or organisations to undertake any activity or to reveal information about any lawful activity. However, an individual or organisation aware of specific unlawful activity may be compelled to divulge what it is that they know of that activity.

**Scope of enforcement provisions and the grant of immunities**

1. All legislation should be drafted such that specific legislated immunities (for example, for journalists, politicians, lawyers, police, etc.) are not required. The law should apply equally to everyone. There should be no such thing as a Journalist Information Warrant (JIW). This could be achieved by having strong "public interest" or "whistle blower" provisions over riding criminal and national security legislation, or perhaps enshrined constitutionally.
2. The secrecy provisions and penalties for disclosure under this and other recent legislation are draconian and akin to the operation of repressive regimes.

   There should be no provision to secretly detain anyone. People detained should have the right to access legal representation or seek independent advice, and to let others (eg. family, friends, media, ...) know of their circumstances. Others (friends, relatives, or anyone else) should not be subject to secrecy provisions regarding the detention of anyone. Others must be free to publicly advocate for the rights of anyone detained by authority under any law applied in Australia.

   There should be no provisions that the subjects of TAR's, TAN's, or TCN's be subject to the secrecy provisions associated with these. There should be no penalty provisions applicable to the subjects of such notices and "requests" unless they are knowingly complicit in undertaking the unlawful activities which are the subject of the investigation.

**Interaction with intelligence agencies other powers**

Espionage and Foreign Interference Bill , Data Retention Act, Telecommunications and Other Legislation Amendment (Assistance and Access) Act (TOLA Act), and consequential amendments to numerous other pieces of legislation, have significantly tipped the balance of power towards the security agencies and infringe the security and privacy rights of law abiding individuals and organisations. The new powers, and their secrecy (and secrecy violation penalty) provisions take Australia ever closer to being a police state where the security authorities can do what they want without fear of scrutiny.

Overall, the entire suite of legislation should be subject to a review to ensure that :

- security agencies cannot act without judicial and ultimately public oversight
- security agencies actions are subject to formal, timely, and public review and reporting
- the privacy and security of law abiding entities is protected
- whistle blowers are strongly protected

**Interaction with foreign laws …. *Clarifying Lawful Overseas Use of Data Act***

- Implementation of capabilities under this legislation would likely conflict with international legislation and industry practices with which Australian companies are required to comply to conduct business (eg. European GDPR, American HIPAA, PCI DSS, …). These typically require entities to:

- Build and Maintain a Secure Networks and Systems
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test
- Protect Data

The TOLA Act can require entities to implement vulnerabilities which will violate the foundations of good software design and system operation. Further, the legislation does not permit sharing of any details of the vulnerabilities so implemented, even within an entity, which further compromises the foundations of good design and operation of the infrastructure critical to the functioning of the world.

- Powers granted under Australian legislation must only be applicable to unlawful activities under Australian legislation (eg. terrorism, fraud, etc.). The powers granted under Australian legislation must not be able to be exercised to investigate activity that is lawful under Australian legislation, but would be considered unlawful in another jurisdiction. For example, it is not clear that the current legislation could not be exercised in conjunction with a foreign entity wanting to investigate for example:
  - a blogger who criticises a member of a royal family or government members of some foreign countries.
  - a woman who has fled a country where adultery is punishable by death.

  Foreign agencies or individuals must not be able to directly exercise or be delegated any of the powers under this legislation. All actions under this legislation must be exercised by Australian authorities and their employees. All information gathered under these powers must be reviewed by Australian authorities and only information specifically relevant to an alleged unlawful activity may be provided to a foreign entity.

**Impact on industry and competitiveness**

Entities subject to this legislation will be disadvantaged in the global market for their products or services. To say otherwise would be hypocritical. Who would want to buy technology or equipment developed in Australia that may facilitate government mandated access to supposedly secure data? Australian technology companies would be treated like Australia (and other Five Eyes countries) has treated Chinese companies like Huawei and ZTE because they could be subject to influence by their government to implement capabilities to circumvent security! Further, it is not clear that an Australian citizen working in an international company would not be subject to the provisions in the current legislation, so who would risk employing Australians?

International developers of software and systems will gleefully advertise that their products are not subject to Australian legislation, and thus have a significant advantage over Australian developers.

There are reports that some of our technology leaders are moving off-shore, or planning to do so because of this legislation.

**Reporting obligations and oversight measures**

This new legislation significantly expands the powers available to law enforcement without providing sufficient public oversight or reporting of how and when such powers have been used. The wording of the legislation is too broad.

Legislation in a democracy should work towards transparency in law, security, business, and society. Secrecy breeds fear, corruption and criminal conduct - it does not reduce it. Australia has some work to do, and I hope that this review will at least make a start restoring the balance between the powers of law

enforcement agencies and the rights of law abiding citizens and organisations. All actions of law enforcement should be transparent, visible, and subject to judicial and public review within strict and sensible time limits.

**Conclusion**

This (and earlier legislation like the metadata retention) legislation threatens the security and economics of the information technology industry in Australia and beyond. It will fail to provide law enforcement with the visibility of content it has sought under it's extensive powers, and threatens the security and safety of law abiding citizens, organisations, and whistle blowers a vibrant democracy should protect.

The government and the security agencies are fond of saying that "if you have nothing to hide, you have nothing to fear". Let us make sure that they also live by that motto.

Regards,

Peter Jardine
(Software Engineer)

**Appendix 1**: My initial submission to the previous review by the Parliamentary Joint Committee on Intelligence and Security of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

9 February 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

The furore over Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 indicates to me that the legislation is seriously flawed, and should be repealed rather than being patched piecemeal.

Whether the legislation requires entities to decrypt communications or circumvent encryption technologies, the effect is the same: Secure communications technologies become insecure.

Entities subject to this legislation will be unable to operate on a global stage. To say otherwise would be hypocritical. Who would want to buy technology or equipment developed in Australia that may facilitate government mandated access to supposedly secure data? Australian technology companies would be treated like Australia (and other Five Eyes countries) has treated Chinese companies like Huawei and ZTE because they could be subject to influence by their government to implement capabilities to circumvent security! There are already reports that some of our technology leaders are moving off-shore, or planning to do so because of this legislation.

The key aspects of this legislation seem to revolve around the requests / demands law enforcement wants to use to compel companies to provide information and / or implement capabilities. These are:

1. TAR (Technical Assistance Request) - a request to "voluntarily"(?) help, such as give technical details about a service.
2. TAN (Technical Assistance Notice) - requires mandatory assistance if the technical capability exists, such as decrypt a specific communication.
3. TCN (Technical Capability Notice) - a company must build new capability to help law enforcement access suspects data, or face fines.

Who is required to pay for the resources (cpu, storage, power, developers, etc.) to comply with these? Diverting company resources to satisfy these requests will divert the company from it’s core business of providing services and technologies it’s customer want to use.

It's not clear how these could be enforced on services developed or hosted outside of Australia - unless we also become more like China and simply ban services from operating in Australia unless they have built in back-doors or other circumventions implemented and accessible to law our enforcement agencies. Such bans will harm Australians in general, and will have next to no impact on the service providers or criminal actors.

Implementation of capabilities under this legislation would likely conflict with international legislation with which Australian companies are required to comply to conduct business internationally (eg. European GDPR, American HIPA, International PCI, …).

Entities subject to this legislation are required to keep secret any capabilities implemented under this legislation. It has been shown time and again that "security by obscurity" is a flawed approach - security

experts have rejected this view as far back as 1851. Big and small companies rely on open algorithms and technologies to secure their business operations in the internet age.

Certainly, there are some aspects of obscurity that are implemented in nearly all organisations to keep their data secure (locked doors, passwords, keys, access control systems, audit trails, ...). However, these are rarely "proprietary". The technologies, methods, and algorithms can be examined and audited without weakening the security of the infrastructure. Security and trust is one outcome of open and rigorous examination. Keeping secret all actions initiated under this legislation is a dangerous path to follow as it does not permit open scrutiny of any measures implemented, potentially leading to severe unintended consequences.

It is worth noting that many companies (like WhatsApp) publish technical details for their service, and many commercially employed encryption schemes are in the public domain. This allows academics, scientists, and anyone else to examine the technology, and potentially identify any weaknesses, which in turn allows the community to evolve to more secure technologies and algorithms, and generally to advance technologically. This legislation would not be able to be imposed on these technologies.

The secrecy and penalty provisions in this (and other National Security) legislation are inexorably leading to the development of a “secret police” regime in Australia. Examples of peoples "*trust*" of “secret police” organisations abound, and will undermine the security of Australia and any trust it's people may still have in the government and the security forces.

Finally, the legislation is fatally flawed in it’s understanding of encryption technology: Any measure implemented can be readily bypassed by even relatively technically illiterate users. One key example of this is that a digital object (file, message, image, program, ...) can be readily and securely encrypted prior to sending it using an application which is known to be insecure (even using using an un-encrypted communication channel!). Anyone trying to intercept such communications will have access to the meta-data (as provided by previous legislation), but will be unable to decipher the content.

This legislation as it stands will not provide security agencies with access to communications of criminal entities – they will quickly migrate to other technologies. The legislation threatens the security and economics of the information technology industry in Australia and beyond.

I submit that this legislation should be repealed (scrapped!).

Any future legislation should work towards transparency in law, security, business, and society. Secrecy breeds fear, corruption and criminal conduct - it does not reduce it.

Regards,
Peter Jardine
(Software Engineer)

**Appendix 2**: My supplementary submission to the previous review by the Parliamentary Joint Committee on Intelligence and Security of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.

12 February 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Supplementary Submission

My initial submission focused on the amendments to the Telecommunications Act 1997 requiring "industry assistance" via the use of TAR's, TAN's, and TCN's. However, the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 touches on a number of other pieces of legislation in addition to the Telecommunications Act 1997 on topics only tangentially related to the industry assistance provisions.

If the entire Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 is not to be repealed, I submit that all of the industry assistance provisions of this act should be repealed, and that the following issues with amendments to ancillary legislation amendments be considered and addressed:

Note that I am a software engineer, and not a lawyer, so I will focus on technical and other broad aspects of the act. I'll leave the finer points of handling irregularities in the warrants, their legal consequences, and officials being able to "not bear an evidential burden in relation to the matters" as specified by the act to more legally qualified submitters.

Amendments to the **Mutual Assistance in Criminal Matters Act 1987**:
Applications by a foreign country for a computer access warrant should be limited to situations where the alleged criminal behaviour is also considered to be serious criminal behaviour under Australian Law (punishable by a maximum penalty of imprisonment for 3 years or more in Australia). The current definition would for example, permit a foreign government to request a warrant to access a the computer(s) of :

- a blogger who criticises a member of a royal family or government members of some foreign countries.
- a woman who has fled a country where adultery is punishable by death.

Furthermore, any data obtained under such a Mutual Assistance warrant must be reviewed by an appropriate Australian authority, and only data relevant to the investigation should be communicated to the foreign country. Agents of the foreign country should never be given direct access to the computer(s) and / or data covered by such warrants. That is, enactment of the warrant and collection of any evidence must be conducted and analysed only by Australian officials.

Amendments to the Surveillance **Devices Act 2004**:
The amendments permit "adding, copying, deleting, or altering other data in the target" (Section 27E What a computer access warrant authorises, paragraph (d)). This provision should have stronger safeguards implemented which ensure that such changes fall strictly under the definition of changes required to implement surveillance measures (paragraph (5) – Certain acts not authorised – needs to be strengthened). This needs to be repeated for paragraphs (7) and (8).

Amendment 99 After subsection 49(2A) (of the Surveillance Devices Act 2004) insert (2B) ...: The inserted (2B) should be better aligned with subsection 49(2). In particular, where (2)(iii) requires details of the kind of device used, (2B) should include details of all additions, deletions, or alterations made under (27E). A computer is not necessarily confined to a premises. (2B) should be better aligned with (2) to include details of any place at which the device was used or located while the surveillance was in effect and state the name, if known, of any person whose location was determined by the use of the computer surveillance.

Amendments to the **Crimes Act 1914**:
The amendments permit "adding, copying, deleting, or altering other data in the target" (Sections 3F(2A)(b), 3F(2B)(b), and 3F(2C) in The things that are authorised by a search warrant). As noted above for similar amendments, this provision requires stronger safeguards. I contend that "adding, deleting, or altering other data" does not fall within the scope of "search" for the purposes of a search warrant. Changes which occur incidentally in the process of normal operation (such as log, audit, and authorisation) should be distinguished from any active adding, deleting, or altering of data under the terms of a search warrant.

Similar protections are required for (the new) sections 3K(5)(b), 3K(6)(b) and 3K(7)

Amendments to the **Customs Act 1901**:
The amendments permit "adding, copying, deleting, or altering other data in the target" (Sections 199(4A)(b) and 199(4B) in The things that are authorised by a search warrant relating to premises). As noted above for similar amendments, this provision requires stronger safeguards. I contend that "adding, deleting, or altering other data" does not fall within the scope of "search" for the purposes of a search warrant. Changes which occur incidentally in the process of normal operation (such as log, audit, and authorisation) should be distinguished from any active adding, deleting, or altering of data under the terms of a search warrant.

Similar protections are required for (the new) sections 199B(2)(b) and 199B(3).

Paragraph 201AA(3)(d). Requires clarification that the removal of data refers to the copy (or copies) of the data created by the investigation, and not the data on the seized equipment itself.

**Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018** –
Requirements for a person to provide information or assistance and Penalties for Offences for non-compliance with said "requests":
Throughout the act, a person (not a member of the security forces) can be "requested" to provide information or assistance to law enforcement officials. These requests of a person are required to be kept secret under threat of (harsh) penalty, and are required to be complied with under threat of (harsh) penalty. Complying with any such request will typically violate security and access control policies of any organisation, will typically result in log and audit entries, and may trigger internal security alerts which will be investigated. Further, the legislation permits "unknown" changes to be implemented by law enforcement officers, which in turn potentially introduces unknown (and un-testable) vulnerabilities into an organisations infrastructure. Any person providing such information or assistance will then likely be subject to disciplinary proceedings within, or dismissal from an organisation. This act has put any such person in an untenable position. These provisions must completely repealed. Any requests for such information or assistance need to be able to be reviewed by information technology peers and any necessary management and / or legal opinions or approvals sought. The person (or organisation) *must* be able to decline such requests without penalty. Any similar provisions in pre-existing computer related legislation should also be repealed. Perhaps the only place such measures could be enforced would be in an organisation that been declared to be an illegal or criminal organisations (eg. some motorcycle gangs, mafia organisations, etc?) by a court of Australia?

Regards,

Peter Jardine.
(Software Engineer)