marshalls+dent
+wilmoth lawyers

# A SHORT GUIDE TO AUSTRALIA'S NEW ENCRYPTION LAWS AND HOW YOUR BUSINESS CAN PREPARE FOR THESE CHANGES*

Early in December 2018, both Houses of Parliament in Australia swiftly passed the controversial *Telecommunications and Other Amendments (Assistance and Access) Bill 2018* (the Bill). The Bill received Royal Assent on 8 December 2018 and is now valid law (referred to as 'the Act' in this article).

A number of security experts have commented that the Act could have significant implications with respect to the invasion of an individual's privacy.

This guide explores some of the key provisions of the Act, how they apply and what businesses and professionals can do to handle these new encryption laws.

## *Am I a 'designated communications provider' under the Act?*

The 'industry assistance' provisions under Schedule 1 of the Act give wide-reaching powers to Australian intelligence agencies and officers of the Federal and State police to issue notices and warrants to a *'designated communications provider'*, compelling it to provide access to authenticated or encrypted communications and data.

Before we go into the different types of notices and orders that can be made under the AA Act, the first question we need to answer is: who is a designated communications provider?

The expansive definition of *'designated communications provider'* has been the subject of many contentious debates amongst government bodies and businesses operating in the technology and communications space. A business (including its employees and contractors) or individual is a designated communications provider if they:[1]

- operate as a phone, telecommunications, software, hardware and internet service provider;
- provide an electronic service that has one or more end-users in Australia;
- operate a website, develop or update a software, or manufacture, supply, install, maintain or operate data processing devices and/or facility;
- connect a facility to a telecommunications network in Australia; or
- repair data processing devices (such as technicians and repairers).

It can then be concluded that this definition of designated communications provider includes almost anyone involved in communication and technology related services, including many start-ups and other fast growing Australian

[1] AA Act, sch 1, s 317C.

businesses who quite reasonably rely on encryption technology and the collection and processing of its customer's data in order to scale.

## *What kind of assistance will I be required to provide?*

The Act sets out a discrete list of 'acts or things' which intelligence agencies can force a designated communications provider to do. Similar to the definition of designated communications provider, the definition of such 'listed acts or things' is broad and grants agencies a potentially invasive list of powers, such as:[2]

- removing one or more forms of electronic protection (including authentication and encryption)[3] applied by a provider;
- providing ***technical information***;
- installing, maintaining, testing and using software or equipment;
- facilitating or providing access to a provider's facility, equipment, data processing device, electronic applications or communications;
- testing, modifying, developing or maintaining a technology or capability;
- substituting a service provided by a provider for another service; and
- concealing the fact that a provider has done any of these acts or things, as long as that provider does not make any "false or misleading statement" or engage in "dishonest conduct".[4]

The term 'technical information' is unfortunately not defined in the Act and thus, may include a wide range of information such as chat logs, source codes, blueprints, technology related data and so on.

## *What kind of technical notices and orders can be issued to me under the Act?*

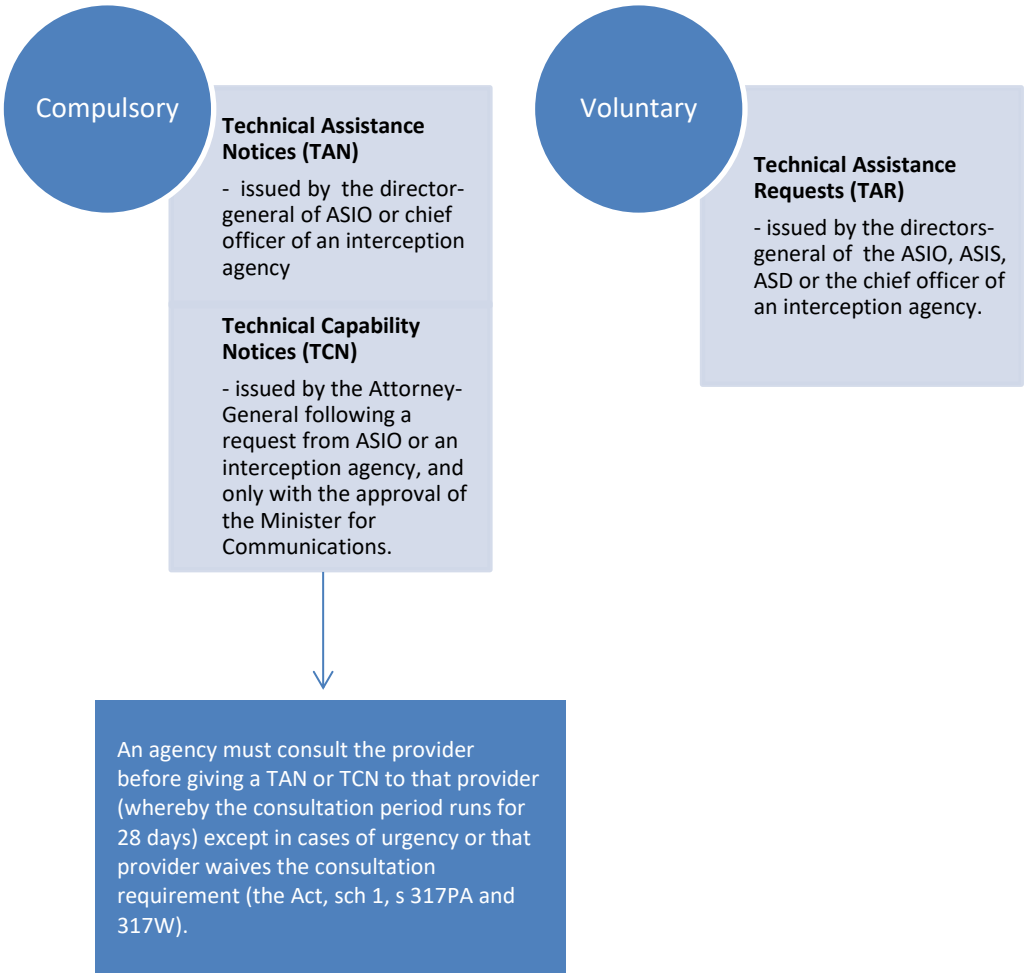
The Act gives two types of power – one afforded to intelligence agencies and the other to law enforcement officers. There is a large overlap between these two powers. As such, we will deal with the intelligence power first.

### Intelligence power

The Act grants intelligence agencies wide-reaching powers to issue the following three orders to compel a designated communications provider to do the above mentioned 'listed acts or things'. These agencies include the Australian Security and Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), and the chief officer of an 'interception agency'.

---

[2] AA Act, sch 1, s 317E(1).
[3] AA Act, sch 1, s 317B.
[4] AA Act, sch 1, s 317E(2).




- A notice must be in writing (unless it is not practicable in the circumstances to do so) and if given orally, it must be recorded in writing within 48 hours.[5] This requirement applies to variations, extensions and revocations of the notices.
- An agency must also, within 7 days after a notice (or a variation, extension or revocation of that notice) is issued to the provider, notify the Inspector-General of Intelligence and Security (IGIS).[6]
- The requirements stipulated in a notice must be proven to be 'reasonable', 'proportionate' and of which 'compliance is practicable and technologically feasible'.[7] The definition of 'reasonable and proportionate' is not defined under the Act, although the scope of 'relevant objectives' as set out below may assist in defining what is 'reasonable and proportionate'

### *Technical Assistance Requests (TAR)*

A TAR is a voluntary notice requiring a designated communications provider to give technical assistance to intelligence agencies for the following *relevant objectives* (which also apply to TAN and TCN):

- safeguarding national security;
- protecting Australia's national security;

[5] AA Act, sch 1, s 317H, 317M and 317TAAA.
[6] AA Act, sch 1, s 317HAB, 317MAB and 317TAB.
[7] AA Act, sch 1, s 317AA, 317P and 317Z.

- enforcing  matters relating to security and integrity of information processed, stored or communicated electronically;
- enforcing the criminal law relating to serious Australian offences; or
- enforcing the criminal law relating to serious foreign offences.[8]

An agency issuing a TAR to a provider must record the notice and advise the provider that compliance with the TAR is voluntary.[9]

### *Technical Assistance Notices (TAN)*

A TAN is a compulsory notice that may compel a designated communications provider to assist the issuing intelligence agency with anything relating to 'listed acts or things' as defined earlier.[10] The directions contained in a TAN focus on a provider's current systems, functions or capabilities.

With a TAN, an agency can demand a provider's assistance with decrypting encrypted data, delete data, accessing, using and altering data so long as such assistance is in relation to the 'relevant objectives' similar to those mentioned in the TAR section.

However, an agency cannot force a provider to build any backdoor capabilities into electronic applications or data processing devices…unless a TCN is issued.

### *Technical Capability Notices (TCN)*

Under the Act, the Attorney-General may, with a request made by an intelligence or law enforcement agency, give a written TCN to a designated communications provider, forcing the provider to build new capabilities (such as backdoors into software and hardware) to assist an agency in carrying out one or more 'listed acts or things'.[11] This means that if a provider operates or develops an electronic application that uses some form of encryption, an agency can require that provider to re-engineer the application or build a new capability that can "decrypt" or "break" the encryption and gain access to the content of a specific communication.

Compared to TAR and TAN, TCN arguably gives the most invasive powers to intelligence and law enforcement agencies to require a provider to carry out surveillance-like and interception activities on their behalf. During the 28-day consultation period, a provider served with a TCN can request an assessment of whether the proposed TCN should be given, and the assessors must be appointed by the Attorney-General.[12]

## Law enforcement power

As an amendment to a number of existing legislations relating to surveillance and interception of communication, the Act affords extensive powers to law enforcement agencies to investigate and gain access to electronic and computer systems with an *assistance order*.[13] An assistance order enables police officers to:

---

[8] AA Act, sch 1, s 317G.
[9] AA Act, sch 1, s 317HAA.
[10] AA Act, sch 1, s 317L.
[11] AA Act, sch 1, s 317T.
[12] AA Act, sch 1, s 317WA.
[13] AA Act, sch 2, s 64A(1).

- access data held in a computer;
- copy data held in a computer; or
- convert data into documentary form.

*Assistance order* is covered under the umbrella Computer Access Warrants (CAW) provisions under the Act, which authorise ASIO and police officers to:

- enter a premise relating to a target computer;
- use the target computer, telecommunications facility, equipment or data storage device at any time to obtain data;
- add, copy, delete or alter data;
- remove a computer from premises; or
- intercept a communication passing over a telecommunications system.[14]

The Act also allows ASIO and law enforcement officers to conceal the fact that any of the above has been done.[15]

## *What are the penalties if I do not comply with a notice or order?*

If a provider does not comply with requirements under a TAN and TNC, the following penalties apply:

- $10 million dollars if the provider is a corporation; or
- $50,000 if the provider is an individual.[16]

In the event of unauthorised disclosure of information about a notice, a person may be subject to a 5-year imprisonment term.[17] A defence in proceedings for a civil penalty, which has been rarely discussed or mentioned, is available to a provider if the provider proves that compliance with a TAN or TCN in a foreign country would contravene a law of that country.[18]

In the case of CAW, a failure to comply with a CAW captures a penalty of approximately $63,000 and a 5-year imprisonment term.[19]

## *I do not need to comply with a notice if…*

A major concern voiced by technology companies and cyber security experts is that by complying with a notice, a 'systemic weakness' or 'systemic vulnerability' will be introduced, therefore jeopardising the integrity of a provider's entire system. Both of these terms are loosely defined in the Act and what they mean in practice remains unknown.

The Act provides that a notice must not have the effect of (a) requiring a provider to build a systemic weakness or vulnerability into a form of electronic protection (such as encryption applications); or (b) preventing a provider from rectifying a weakness or vulnerability caused by a notice.[20]

---

[14] AA Act, sch 2, s 27E(1)-(2).
[15] AA Act, sch 2, s 27E(7).
[16] AA Act, sch 1, s 317ZB(1).
[17] AA Act, sch 1, s 317ZF(1)(e).
[18] AA Act, sch 1, s 317ZB(5).
[19] AA Act, sch 3, s 9.
[20] AA Act, sch 1, s 317ZG.

When assessing the nature of modern technology and cyber security strategies, it becomes difficult to formulate a scenario where a notice would not force a provider to implement a systemic weakness or vulnerability to their existing system. It's a catch-22 situation and a challenge to envisage an appropriate and objective framework that can ensure compliance is 'practicable' or 'technically feasible' in this context.

## *What if my customers are affected by a security or data breach as a result of my compliance with a notice?*

The 'Immunity' provision in the Act states that a provider, its officer, employee or agent are not subject to any civil liability for anything done in compliance with a TAN or TCN.[21] This exemption does not apply to a TRN unless the provider's voluntary compliance is capable of 'giving help' to an agency.[22]

The biggest issue with this defence is that the Act, as mentioned earlier, prohibits a provider from disclosing (by making a press release or social media announcement) to the public that a data or security breach occurs as a result of their compliance with a notice. This means that a provider's reputation from a public relations perspective may already be affected by the time the gag order is removed by the agency. Another detrimental effect of the Act is that international corporations now need to think twice before engaging Australian employees and contractors, given that an agency can compel anyone classified as a 'designated communications provider' to follow an order.

Our recommendations set out below will cover a number of options and strategies for businesses to minimise the impact of these new laws.

## *Recommendations*

For businesses based in Australia and fall within the scope of the Act, we recommend the following measures and strategies to be put in place:

- conduct a thorough review and assessment of your data management practices to ensure that stringent protection measures are in place;
- if you consider implementing some form of encryption in the course of conducting your business, consider using an international third party provider who cannot be compelled by an Australian government body to comply with a notice;
- review and update your terms and conditions, privacy policies, terms of use and any other client-facing documents to ensure that they inform the customer of your new obligations and the types of information that must be disclosed to a law enforcement body should the business be served with a notice;
- create a mechanism whereby customers actively agree to not hold the business liable for any damages or losses relating to a notice and that the business reserves the right to terminate the agreement with customers in the event a notice is issued (this can be part of your service agreement or website/app terms and conditions);
- update your employment or contractor agreements to ensure that an employee or contractor has not been served with a notice prior to the date of agreement;

[21] AA Act, sch 1, s 317ZJ.
[22] AA Act, sch 1, s 317G.

- if you are a contractor or service provider in Australia, update your pro-forma agreement to ensure that the principal releases you from any liability to the principal in the event you are served with a notice;
- consult your insurer to discuss the financial implications of these laws;
- discuss potential issues and concerns with a law firm and cyber security experts; and
- if you are served with a TAN or TCN, ensure that you consult a lawyer during the 28-day period to understand your obligations and compliance procedures.

*marshalls+dent+wilmoth has lawyers who can assist you to navigate the changing business and technology landscape. Please do not hesitate to contact us on (03) 9670 5000.*