'Going dark': the unprecedented government measures to access encrypted data

BY ARTHUR KOPSIAS APM

Arthur Kopsias APM is a solicitor, NSW Police Force and a member of the Law Society's Privacy Law Committee.

Snapshot

- The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* became law on 8 December 2018.
- It introduces a number of measures designed to address the ongoing problem faced by agencies of 'going dark' in order to access the meta data of terrorist suspects.
- The Act creates a new industry framework for law enforcement and security agencies to access data and content held by designated communications providers within or outside the Australian jurisdiction.
- The Act has implications (and perhaps unforeseen ramifications) for the operation of the United States' *CLOUD Act 2018*.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 was introduced to Parliament by the Minister for Home Affairs on 20 September 2018, sparking enormous national interest. The Attorney-General subsequently referred the Bill to the Parliamentary Joint Committee on Intelligence and Security ('**PJCIS**') for inquiry and report. The Inquiry received submissions from the Law Society of NSW, the Law Council of Australia, a large number of other commercial and private legal institutions, carrier industry providers, government, NGOs and law enforcement and security agencies.

On 8 December 2018 the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* ('***TOLA Act***'), received royal assent and became law. The reason given for the rapid passage of such complex and significant reforms, was reportedly a heightened risk of terrorist incidents over the Christmas and New Year period.

Encryption

Thanks to the internet, the encryption of modern electronic communications is critical. It allows us to communicate securely, privately and confidentially in many forms of communication and online activities. Thus the ability to encrypt and subsequently decrypt communications is integral to almost every online activity, from chatting on a mobile phone, using social media, accessing commercial, retail or government services such as Centrelink, online banking, shopping and web browsing. Therefore, it is important to ensure that communications are secure and private, and are not weakened to hinder or disrupt the normal activities undertaken by law-abiding citizens.

The greatest benefit of encryption also creates the biggest problem. In this context, the evolving digital environment presents an increasing challenge for law enforcement and national security agencies. Secure, encrypted communications are being used by terrorist groups and organised criminals to avoid detection and disruption, and the inability to read or understand encrypted communications – colloquially referred to as 'going dark' – has presented real challenges for agencies worldwide. Over 90 per cent of telecommunications information being lawfully intercepted by the Australian Federal Police now uses some form of encryption. Malicious actors increasingly communicate through secure messaging applications, social media and Voice over Internet Protocol ('**VoIP**') services (see Submission 18, Department of Home Affairs, p3).

The framework

Schedule 1 of the new *TOLA Act* inserts Part 15 – 'Industry Assistance', into the *Telecommunications Act 1997* ('***Telco Act***'). The Part creates a new framework for industry assistance and intends to complement the existing obligations of Carriers/ Carriage Service Providers ('**CSP**s') to provide reasonable assistance to law enforcement and security agencies under s 313 of the *Telco Act*.

This 'Industry Assistance' framework in Part 15 contains three distinct new powers which allow an agency head or their delegate to issue, or seek the issue of, a:

- ***'technical assistance request' (TAR)*** *for voluntary assistance.* This grants civil immunity and limited criminal immunity for any assistance provided.
- ***'technical assistance notice' (TAN)*** *for compulsory assistance.* This power is to be used to request the assistance which a designated communications provider is already capable of providing.
- ***'technical capability notice' (TCN)*** *for new capabilities.* This notice can only be issued by the Attorney-General and requires a provider to create a specific capability where the provider is not currently able to assist.

Assistance from designated communications providers

The term 'designated communication provider' ('**DCP**') is broadly defined and intended to capture a wide range of entities integral to the modern Australian communications market. While many of these providers are based within Australia, equally many are not, so the Act also applies to offshore entities who operate or supply communications services, devices or products for use within Australia. Section 317C of the amended *Telco Act* contains a full list of DCPs. These include:

- carriers and CSPs and anyone who facilitates the services of Carriers/CSPs e.g. Telstra, Optus, Vodafone;
- electronic service providers (with at least one end-user in Australia) and anyone who facilitates the services of electronic service providers, e.g. Facebook, Google and Amazon Web Services; and
- manufacturers of electronic equipment and anyone who facilitates the manufacture of electronic equipment (likely to be used in Australia) e.g. Samsung, Nokia.

Civil immunity is available for DCPs acting in good faith to ensure they are protected from any legal risk (*Telco Act*, s 317G(1)).

What kind of assistance may authorities seek from a communications provider?

Section 317E sets out the 'acts' or 'things' that may be sought from a DCP. These include, but are not limited to: removing one or more forms of electronic protection; providing technical information; facilitating access to services and equipment; installing software; modifying technology; and concealing that the company has done any of the above. An intelligence or interception agency could, for example, send a criminal suspect a notification to update messaging software that in fact allows the intelligence or interception agency access to their messages. It is important to note that a DCP listed in s 317C can only be asked to do things connected to what the legislation calls the provider's 'eligible activities'.

Who can authorise the use of the powers?

The use of the powers has been restricted to the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation ('**ASIO**'), the Australian Secret Intelligence Service, the Australian Signals Directorate, and State and Territory Police forces.

The Act provides that the head of each agency may issue a TAR or a TAN, or may delegate these functions to an appropriate senior official in their organisation (s 317ZN to 317ZR). A TCN may only be issued by the Attorney-General in accordance with any guidelines provided for in s 317S (if any).

What access authority is required?

Access using a TAR, TAN or TCN (defined earlier) will be restricted to agencies already having or obtaining a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979*, the *Surveillance Devices Act 2004*, the *Crimes Act 1914* (Cth), or any law of a state or territory (s 317ZH). These provisions are therefore not intended to circumvent other established legal and regulatory processes through which agencies are able to obtain meta data and content.

Purpose of the agencies' powers

The use of the powers is connected to the lawful functions and activities of the agency issuing the notice or request e.g. ASIO safeguarding national security or State/Territory and Commonwealth police enforcing the criminal law so far as it relates to serious Australian or foreign offences (s 317(d)(e)). A serious offence is defined as 'an offence against a law that is punishable by a maximum term of 3 years imprisonment, or more or for life' (s 317B).

What must decision-makers take into account?

Before issuing a TAR or TAN, the decision-maker must be satisfied of certain matters and turn his or her mind to specific criteria. The decision-maker must be satisfied that the request or requirement is reasonable and proportionate and that compliance is practicable and technically feasible (see s 317JAA for TARs and s 317P for TANs).

In determining whether a request or notice is reasonable and proportionate, the decision-maker must have regard to: the interests of national security; the interests of law enforcement; the legitimate interests of the relevant provider; the objectives of the request or notice; the availability of other means to achieve these objectives; whether the requirements are the least intrusive form of industry assistance insofar as it might impact innocent third parties; privacy etc (see s 317JC for TARs and s 317RA for TANs).

Similarly, for a TCN, the Attorney-General must not issue a TCN unless satisfied that the requirements imposed by the notice are reasonable and proportionate and that compliance with them is practicable and technically feasible (s 317V). In determining whether the requirements of a TCN are reasonable and proportionate, the decision-maker must have regard to all of the matters outlined above and other factors (s 317TAAA(6)).

Systemic weaknesses and vulnerabilities

Section 317ZG ensures DCPs cannot be required to 'implement or build [or rectify] a systemic weakness, or systemic vulnerability, into a form of electronic protection' (also called 'backdoors' for encryption mechanisms).

Many submissions received by the PJCIS from industry providers, legal and regulatory associations, expressed concern over the privacy aspects, the costs of compliance for DCPs, and that neither the term 'systemic weakness' or 'vulnerability', nor the term 'electronic protection' was sufficiently defined in the draft Bill. It is unclear at what point a requested weakness would become systemic, i.e. would a weakness be systemic when a certain system is involved or does the concept of systemic vulnerability revolve around the number of users (potential or actual) affected by the weakness and, if so, what would a relevant user number threshold be? It is also unclear how vendors of telecommunications network equipment could be required to do a specified act or thing without introducing a systemic weakness or vulnerability given that their products are at the core of most digital communications (see 15, Joint Submission 2.6, p15).

No profit/no loss compliance

If a DCP is compelled to provide assistance, they shall do so on the basis that they neither profit nor lose money – which basically includes the direct costs involved in providing that assistance (unless an independent applications costs negotiator otherwise agrees or determines it is against the public interest) (see s 317ZK(2)).

Enforcement

The framework is not intended to be adversarial. It is built on the spirit of co-operation, as many providers in this jurisdiction already provide assistance and are willing to do so.

However, if a DCP refuses to comply, enforcement proceedings may be instituted before the Federal Court as set out in Division 5. The civil penalty for contravention is 47,619 points (approx. $10 million) for corporate entities and 238 points (approx. $50,000) for private individuals (Division 5 Section 317ZB).

Consultation requirements

Before a TCN is issued, there is a mandatory 28-day (minimum) consultation period. The requirement to consult will not apply if the Attorney-General is satisfied that: the TCN should be given as a matter of urgency, compliance with the consultation requirement is impracticable or it is waived with consent from the provider (s 317W). The spirit of the framework suggests that as a matter of best practice and to minimise the risk of any adverse impact on providers or the wider public, consultation should be undertaken at all stages, regardless of whether it is a TAR, TAN or TCN.

How are these powers oversighted?

The use of industry assistance powers is subject to requirements that either the Commonwealth Ombudsman or Inspector-General of Intelligence and Security (depending on the agency using the powers), be notified and that agencies comply with oversight requirements. The inspection powers of the Commonwealth Ombudsman are listed in s 317ZRB.

Are there reporting requirements?

The use of industry assistance powers is subject to annual reporting requirements. Interception agencies must notify the Home Affairs Minister of their use of the industry assistance powers throughout the year ending 30 June including the number of notices issued and those in relation to the enforcement of an Australian offence with a penalty of three years or more imprisonment.

Implications of the United States *CLOUD Act*

With the extraterritorial operation of the amended *Telco Act*, it is important to discuss its intended correlation with the US *Clarifying Lawful Overseas Use of Data Act* ('***CLOUD Act***').

The *CLOUD Act* was passed on 23 March 2018 as part of the *Vehicle for Consolidated Appropriations Act 2018* (US).

Prior to the *CLOUD Act*, foreign nations seeking data in the United States generally were required to request the assistance of the US government either through procedures established by mutual legal assistance treaties ('**MLATs**') or judicial requests known as letters rogatory.

In *United States v Microsoft Corp* (No 17-2,584) (2018), the Supreme Court of Appeal was set to address whether the United States could compel Microsoft to release emails housed in a data centre in Ireland through a warrant issued under the *Stored Communications Act* ('***SCA***'), when Congress passed the *CLOUD Act* as part of the *Consolidated Appropriations Act 2018*. It thereby amended the *SCA,* requiring service providers to release data in their possession, custody, or control regardless of whether the data is located in or outside the United States.

The *CLOUD Act* creates a framework for the US to enter into executive agreements with qualifying foreign governments for reciprocal cross-border access to data, and creates the conditions by which a country can be considered a qualifying foreign government.

Mutual legal assistance treaties

The *Mutual Assistance in Crime Matters Act 1987* is the vehicle by which the government can request mutual legal assistance from foreign countries for criminal investigations, prosecutions and proceeds of crime, in accordance with Australia's bilateral Mutual Legal Assistance Treaties ('**MLATs**'). However, the process is often undermined by challenges in timely access to data, with requests for assistance sometimes taking up to twelve months. This delay can have a significant impact on the investigation and prosecution of serious crimes, such as terrorism and organised criminal activity.

The Minister for Law Enforcement and Cyber Security, Mr Angus Taylor, has said that the US *CLOUD Act* will 'greatly improve the efficiency of law enforcement's access to the information they need to do their job and strengthen protections

The greatest benefit of encryption also creates the biggest problem. In this context, the evolving digital environment presents an increasing challenge for law enforcement and national security agencies. Secure, encrypted communications are being used by terrorist groups and organised criminals to avoid detection and disruption, and the inability to read or understand encrypted communications – colloquially referred to as 'going dark' – has presented real challenges for agencies worldwide.

of people's data, no matter where their data is held.' (https://www.arnnet.com.au/article/635859/government-throws-support-behind-new-us-data-law/). It is believed an executive agreement between Australia and the US would complement the Australian *TOLA Act*, as it would have the practical effect of allowing law enforcement agencies reciprocal rights to serve lawful access warrants, expediting the evidence-gathering process for serious criminal investigations and prosecutions.

On 7 December 2019, Law Council of Australia President Morry Bailes stated that while the encryption access legislation that was rushed through the Senate is an improvement on the original Bill, there is now the very real possibility of unintended consequences as well as intelligence agency and law enforcement overreach.

Computer Access Warrants

Schedules 2 and 3 of the *TOLA Act* deal with 'Computer Access Warrants' which apply a similar framework to the extra-territorial operation of the Act for agencies accessing data/content on local and overseas servers and other computer/devices – something which might be a topic of further interest and discussion amongst the legal community, but which is beyond the scope of the present article.

Parliamentary Joint Committee on Intelligence and Security

Notwithstanding the fact that the *TOLA Act* is now law, it is still subject to ongoing review, with public submissions invited. The PJCIS is expected to complete its review by 3 April 2019. **LSJ**

* To learn more from Mr Kopsias about the implications of this controversial legislation, as well as other important developments in criminal law, practitioners are invited to attend the Law Society's upcoming **Criminal Law half day intensive CPD seminar on Tuesday 19 February 2019.** For more details about the various topics and speakers, go to:

www.lawinform.com.au