Assistance and Access Bill 2018 – Australia's new motion to enable decryption of encryption

21 August 2018

Authors: Mike Grace, Hugo Chan, Susanna Su, Renee Xue

Explore more insights 365

In brief

On 14 August 2018, the Federal Government released its long-awaited *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (the **Bill**). The Bill seeks to provide Australian law enforcement and national security agencies with broader powers to access encrypted data stored in communication devices. The Government's concern is that the growing use of encryption in these devices has significantly reduced the ability of law enforcement and security agencies to carry out investigations.

The Bill introduces three key overarching reforms:

1. broadening the obligations of both domestic and foreign 'designated communication providers' to assist law enforcement and security agencies to access certain communications – 'designated communication providers' include carriers, carriage service providers, device and component manufacturers, application and software providers;

2. establishing new computer access warrants that allow agencies to covertly search and obtain evidence directly from devices; and

3. strengthening the ability of existing law enforcement and security authorities to overtly access data through search and seizure warrants.

The Bill is intended to align Australia's laws with those of the UK and the US which have provided law enforcement agencies with similarly broader powers to require assistance from industry to access user data to tackle terrorism and national security related crime and issues.

Public consultation on the Bill is open until 10 September 2018.

In detail

Background to the Bill

The Explanatory Document to the Bill states that 95 per cent of the Australian Security Intelligence Organisation's (**ASIO**) most dangerous counter-terrorism targets use encrypted communications. The Minister for Law Enforcement and Cyber Security, Angus Taylor, has also commented that in the last 12 months, 200 investigations of serious crimes were impeded due to inability to access and decrypt encrypted data.

Through this Bill, the Government has clearly expressed desire to overcome technical barriers to enable its law enforcement and security agencies access to what it views as key sources of information crucial to public safety and security.

An overview of the key proposed changes

1. Industry assistance framework

A new Part 15 will be inserted into the *Telecommunications Act 1997* (Cth) to create an industry assistance framework enabling certain government agencies access to encrypted data and devices.

This framework includes:

- **Technical assistance request:** ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate and interception agencies **can require voluntary assistance** from designated communications providers to aid in the performance of their core functions related to enforcement of criminal law and protecting national security.

- **Technical assistance notice:** where a designated communications provider is unwilling to provide voluntary assistance, the Director-General of Security or a head of an interception agency **can require assistance that is reasonable, proportionate, practicable and technically feasible**, if the provider is already capable of providing that assistance. This includes situations where there is no end-to-end encryption and the provider holds the encryption key.

- **Technical capability notice:** where a designated communications provider is not capable of providing assistance, the Attorney-General can require the provider to build a new capability in order to provide that assistance. Any request must be **reasonable, proportionate, practicable and technically feasible**, and the provider must have been consulted before the issue of a technical capability notice.

2. New computer access warrants

Proposed amendments to the *Surveillance Devices Act 2004* (Cth) will create a new class of computer access warrants allowing law enforcement agencies to search and access content on electronic devices. The powers included in a computer access warrant are broad and may include:

- entering premises and removing a computer from premises to execute a warrant;

- intercepting data to execute a warrant (the use of intercept data requires an additional interception warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth) – this is waived for ASIO under new powers, unless it is using the information for its own purposes); and

- concealing access (while the warrant is in force, within 28 days of it ceasing, or the earliest time at which it is reasonably practicable).

While a computer access warrant is in force, a law enforcement officer may apply to a judge or Administrative Appeals Tribunal member for an order compelling reasonable and necessary assistance from a person with knowledge of the device.

3. Enhanced search warrants and ASIO assistance powers

Schedule 3 of the Bill will amend the *Crimes Act 1914* (Cth) to allow law enforcement agencies to remotely collect evidence from electronic devices under an overt warrant instead of having to physically go onto the premises, as required under the current law. It will also introduce a new definition of 'account-based data' which will allow agencies to access data from online accounts associated with those devices (e.g. Facebook or email).

Schedule 3 will also amend section 3LA of the *Crimes Act 1914* (Cth) to enable law enforcement agencies to apply for court orders to compel certain individuals to assist in giving access to devices found both within the warrant premise and during an in-person search. Schedule 4 of the Bill will amend the *Customs Act 1901* (Cth) by providing the Australian Border Force (**ABF**) with the power to apply for a search warrant to use computers or other data storage devices to access data in order to determine whether the relevant data is evidential material.

Finally, Schedule 5 of the Bill will amend the *Australian Security Intelligence Organisation Act 1979* (Cth) to provide greater assistance powers to ASIO in the performance of its functions. For example, section 21A(1) provides a protection from civil liability for a person that voluntarily assists ASIO following a request made by the Director-General, subject to certain limitations.

Consultation

There is much to consider in this Bill, and it will take time to fully comprehend the extent of the Bill's wide ranging effects.

Public consultation on the Bill is open until 10 September 2018 and the Bill can be viewed here.

Let's talk

For a deeper discussion of how these issues might affect your business, please contact:

Cameron Whittfield, Melbourne
+61 (3) 8603 0140
cameron.whittfield@pwc.com

Adrian Chotar, Sydney
+61 (2) 8266 1320
adrian.chotar@pwc.com

Joni Henry, Sydney
+61 (2) 8266 2444
joni.henry@pwc.com

Tureia Sample, Sydney
+61 (2) 8266 5253
tureia.sample@pwc.com